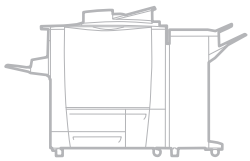


ColorQube™ 9201/9202/9203

System Administrator Guide

xerox

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Document Version: 1.0 (05/09).

Table of Contents

1 Introduction

This guide has been created for System Administrators who need to install, set up and manage printers and other services on their network.

To use the procedures in this Guide effectively, System Administrators must have previous experience working in a network environment and must possess Supervisor, Administrator, Account Operator, or equivalent rights to the network. They must also have prior knowledge of how to create and manage network user accounts.

Xerox ColorQube™ Series

These models have copying, printing, scanning and faxing capabilities. The devices supports scanning too and has the capability of storing print, copy and scan files on the device. It copies and prints at 30/40/50 pages per minute depending on the model.

A Document Feeder, Bypass Tray and Paper Trays 1, 2 and 3 are supplied as standard.

	ColorQube™ 9201	ColorQube™ 9202	ColorQube™ 9203
Digital Copying	Standard	Standard	Standard
Network Printing	Standard	Standard	Standard
Scanning	Standard	Standard	Standard
E-mail	Standard	Standard	Standard
Fax	Option	Option	Option
Paper Tray 1, 2 & 3	Standard	Standard	Standard
High Capacity Feeder	Option	Option	Option
Offset Catch Tray	Option	Option	Option
80 GB Hard Drive	-	Standard	Standard
USB Thumb Drive	Standard	Standard	Standard
Low Capacity Stapler Stacker (LCSS)	Option	Option	Option
High Volume Finisher (HVF)	Option	Option	Option
HVF with Booklet Maker / Post Processor & Trifolder	Option	Option	Option

	ColorQube™ 9201	ColorQube™ 9202	ColorQube™ 9203
Foreign Device Interface	Option	Option	Option

Related Information Sources

Information available for this product series consists of:

- The *System Administrator Guide* (this guide)
- The *Quick Use Guide*
- The *Interactive User Guide*
- The *Advanced User Guide*
- The Xerox website *www.xerox.com*

Customer Support

If you need assistance during or after product installation, please visit the Xerox website for online solutions and support:

http://www.xerox.com

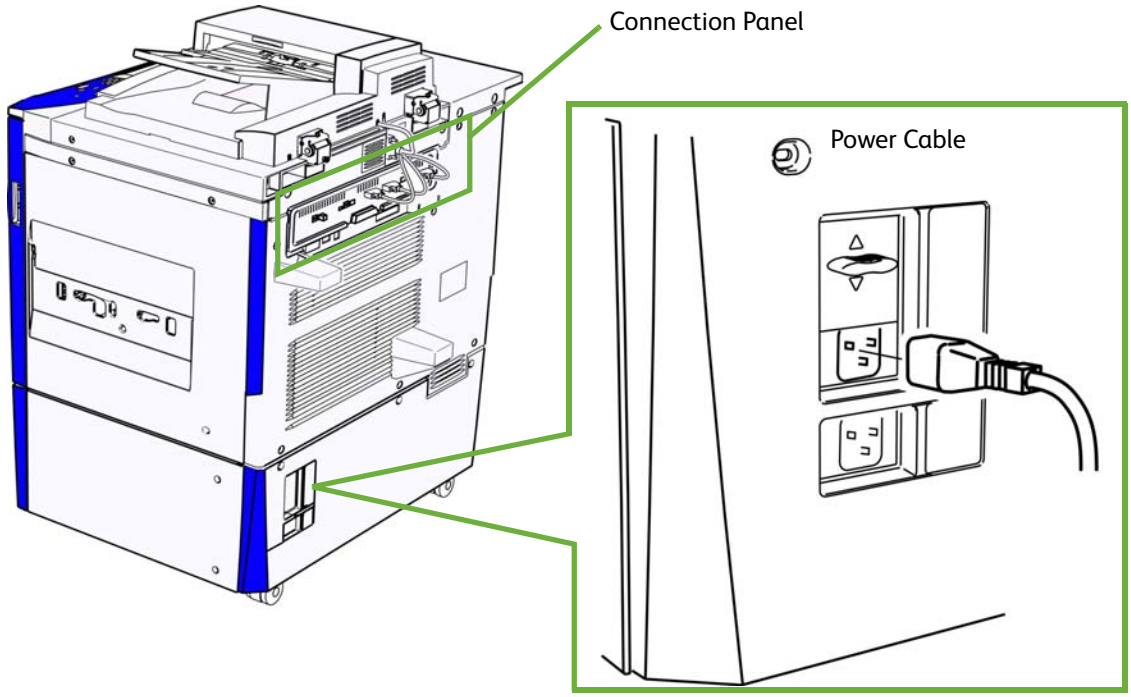
2 Device Connection

This chapter describes how to connect your device to a network and configure Ethernet settings.

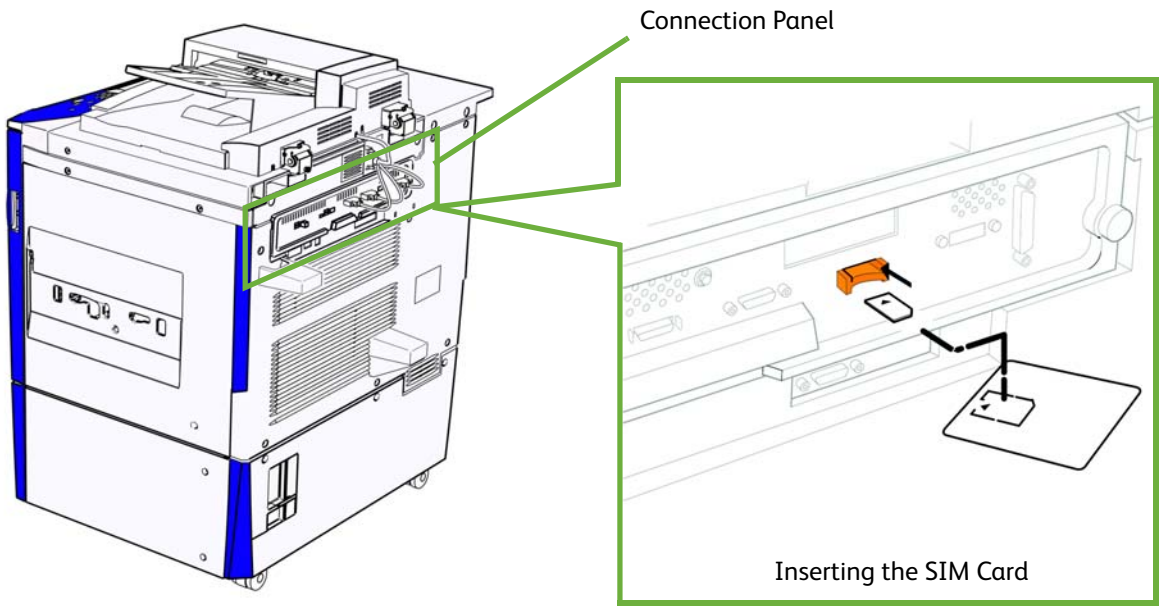
Front View

Power On/Off Switch

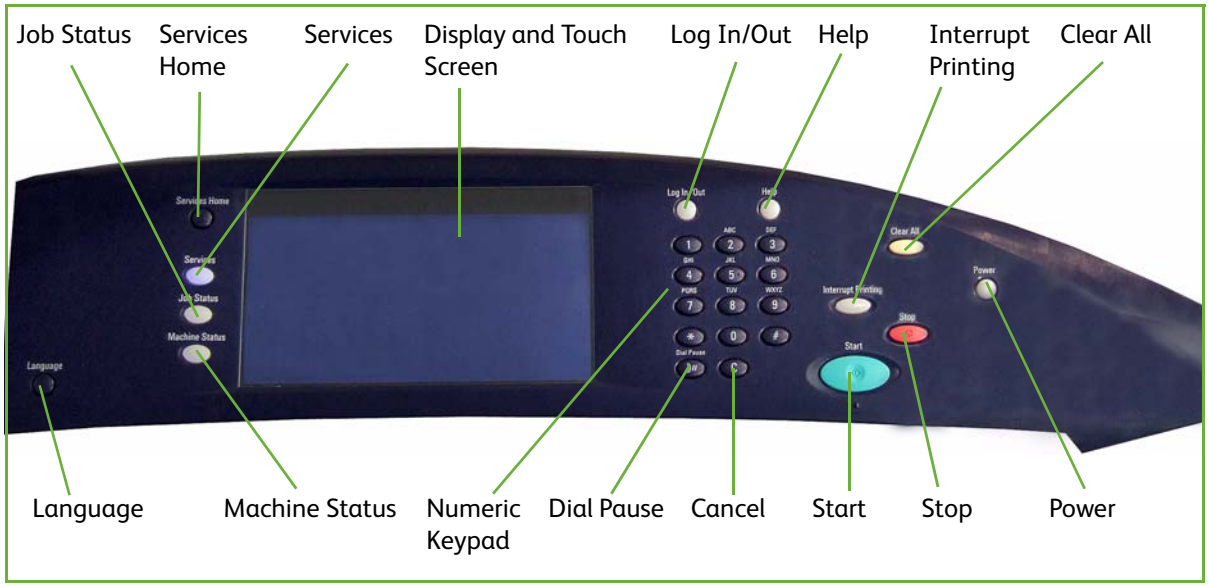
Rear View



Inserting the SIM Card



Device Control Panel Overview



Initial Connection

Follow these steps to physically connect your device to the network.

1. Connect the Power Cable
   Ensure the device is connected to a suitable power supply and that the power cord is fully plugged in to the electrical outlet.
2. Connect the Ethernet Cable
   Connect a 10/100/1000 BaseT Ethernet cable to the Ethernet port at the rear of the device and the other end of the cable to your network port.
3. Insert the SIM Card
   Insert the SIM Card before powering On the device, the SIM slot is located at the rear of the device.
4. Power On the Device
   The Power On button is located at the left-side of the device.

The Welcome Page and Installation Wizards

An Installation Wizard displays the first time the device is powered on, providing the ability to set the date and time.

Simultaneously, a Welcome Page is enabled as the opening page of the device's Internet Services web pages. You can click **[Configure Device]** on this Welcome Page, or click the Configuration Overview link on the Properties tab, to go directly to the Install Wizards for configuring protocols and optional services.

A **[I Have a Cloning File...]** button on the Welcome Page lets you copy configuration settings from a compatible Xerox system and apply them to this system.

To stop displaying the Welcome Page, check the **[Don't Show Welcome Page Again]** box.

To access the Welcome Page or Properties tab of Internet Services, TCP/IP and HTTP must be enabled on the device as described in the Introduction on page 1-1 of this guide.

Complete the Installation Wizard

If this is the first time the device has been powered on, the **Installation Wizard** will run. If this screen does not appear, proceed to **Network Connectivity** in this chapter.

1. At the Installation Wizard screen, touch **[Next]**.
2. Verify the Customer Support Telephone number, or input the correct entry by touching the box and entering the number by pressing the numbers on the keypad. Touch **[Next]**.
3. Set the date format required. Touch **[Next]**.
4. Set the date by touching the buttons and pressing the numbers on the keypad. Touch **[Next]**.
5. Set the clock format. Touch **[Next]**.
6. Set the time, touch **[Next]**.
7. Set the Greenwich Meantime Offset according to the country you are in. Touch **[Next]**.
8. A screen will appear to indicate that you have successfully completed the Xerox Installation Wizard. Touch **[Finish]**. The device will save the settings and reboot. If enabled a configuration report will print.

Administrator Access

The **<Log In/Out>** button provides access to the Administrator Tools area. Administrator access is required to change settings such as network information on the device.

1. Press the **<Log In/Out>** button on the Control Panel.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, then touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch the **[Tools]** tab.

Print a Configuration Report to Verify Current Device Settings

> Note
> A Configuration Report should have printed when the device was powered off, then on, during Power Cable and Ethernet Cable installation. If necessary, perform the following steps:

1. Press the **<Machine Status>** button on the device.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

Ethernet Configuration

Ethernet Port

The Ethernet Interface is set to auto detect the speed of your network. The device supports the following selectable speeds:

- Auto
- 10Mbps Half-Duplex
- 10Mbps Full-Duplex
- 100 Mbps Half-Duplex
- 100 Mbps Full-Duplex
- 1 Gbps Half-Duplex.
- 1 Gbps Full-Duplex

Note

If your network has hubs that have Auto-Sensing enabled and the device Ethernet speed is set to Auto, it is possible that the hub will not arbitrate to the correct speed.

Setting the Ethernet speed at the device

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, then touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch **[Tools]**.
5. Touch **[Network Settings]**.
6. Touch **[Advanced]**, if a warning message appears, touch **[Continue]**.
7. Touch **[Ethernet Physical Media]**.
8. Select the *Speed* to match the speed set on your hub or switch.
9. Touch **[Save]**, touch **[Close]**.
10. Press the **<Log In/Out>** button.
11. Touch **[Confirm]** to exit the Tools Pathway.

Enable TCP/IP and HTTP at the Device

Look at the Configuration Report, verify whether the addressing shown under TCP/IP Settings will enable this device to communicate over your network. Also, verify that HTTP is enabled under HTTP Settings, to enable use of the device's web user interface for network and options configuration. If necessary, reset TCP/IP addressing (including DHCP and DNS settings) and enable HTTP as follows:

1. Go to the device and press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, then touch **[Enter]**.
   Tip: This password can be changed by following the steps provided in the Administrator Tools topic in the General Setup section of this guide.

3. Press the **<Machine Status>** button, and then the **[Tools]** tab.
4. Wait for the screen to refresh, touch **[Network Settings]**, touch **[Advanced]**, if a warning message appears, touch **[Continue]**.
5. Touch the **[HTTP Settings]** button, touch **[Enable]**, touch **[Save]**, then touch **[Close]** to return to the Network Setting screen.
6. Touch **[TCP/IP Settings]**.
7. Configure TCP/IP settings, including DHCP (Dynamic Addressing) and DNS, touch **[Save]**, touch the **[Close]** button to return to the Network Setting screen.

   Note

   This device supports IPv6 addressing, with an automatically-built Link Local Address for broadcasting to routers that can supply the network-layer configuration parameters. See Configure Protocols with Internet Services on page 2-9.

Quick Setup

When your device is configured with an IP address and HTTP is enabled, you can configure network information from your web browser via Internet Services. Enter the IP address of the device in your web browser to access Internet Services.

CentreWare Internet Services

CentreWare Internet Services is the embedded HTTP server application that resides in the device. Internet Services allows Administrators to change network and system settings on the device from the convenience of their desktops.

Many of the features available within Internet Services will require an Administrator User Name and Password. The default User Name is **admin** and the default Password is **1111**. A user will only be prompted for an Administrator's User Name and Password once in a single browser session.

System Configuration

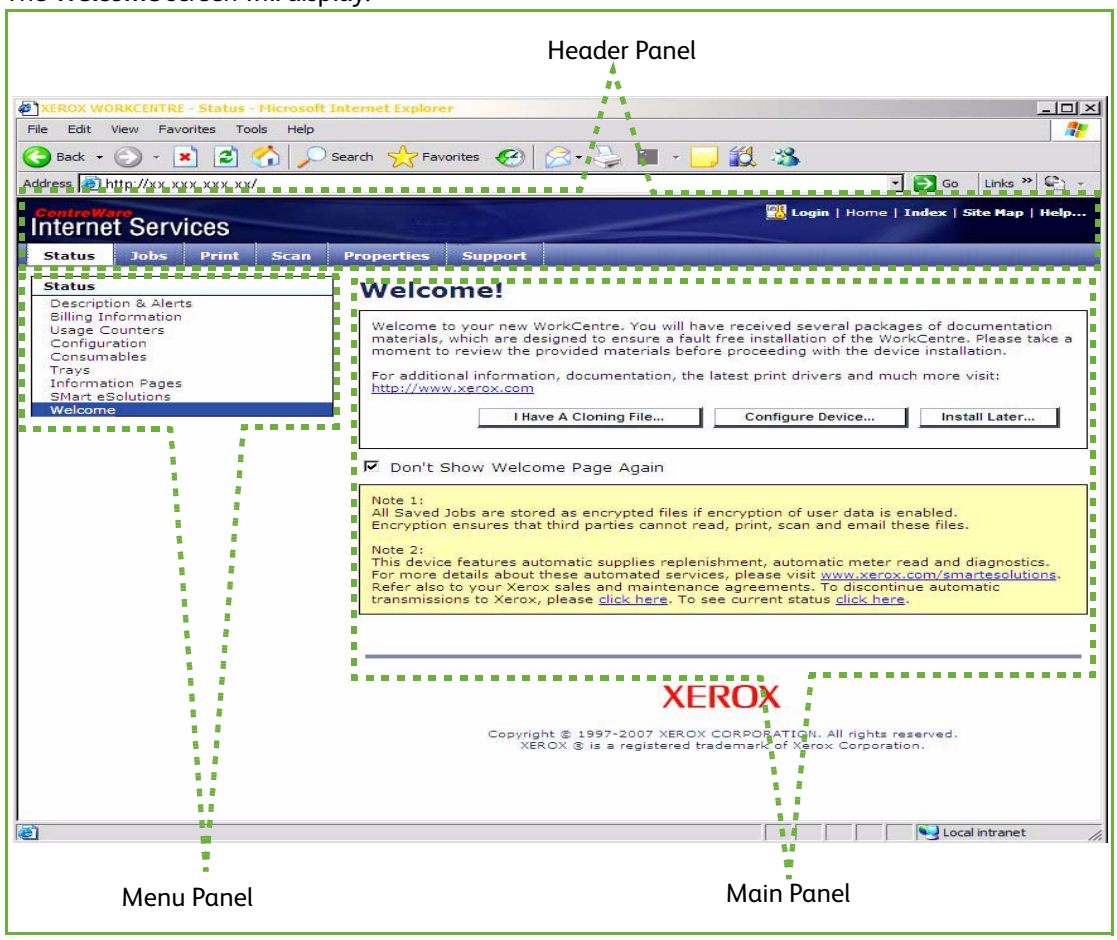
To use CentreWare Internet Services, you need to enable both TCP/IP and HTTP on the device. See How to Add or Change a Static IP Address when there is no DHCP Server Available on page 2-9.

Access Internet Services

To view the **[Internet Services Welcome]** screen:

1. Enter the device's *IP Address* in the web browser.
2. Press **[Enter]** or click on the **[Go]** button. For example:

The **Welcome** screen will display.



The Internet Services home page contains three panels without visible boundaries. You can change the left and right panel sizes by dragging the boundary between them.

- **Header Panel:** displays the header for all pages. The header includes the CentreWare Internet Services logo and model of the device. The header for the ColorQube series also includes a user mode icon, and the name or type of a logged-in user. Just below this panel on most pages is the tab bar which corresponds to the five functions or page buttons. These are **[Status]**, **[Jobs]**, **[Print]**, **[Scan]**, **[Properties]**, and **[Support]**. You can navigate through the pages when you click the text on each tab.
- **Menu Panel:** Displays a navigation tree, listing the items available within each category, with the currently displayed item highlighted.
- **Main Panel:** Displays information and settings for an item selected on the Menu Panel.

When you open Internet Services, a welcome screen is displayed. If you click the **[Configure Device...]** button, a Configuration Overview screen opens which provides links to the printing protocols and services that you can configure on the device.

If you click the **[I have a Cloning File...]** button, you can copy settings from one device and transfer them to another device with the same version of system software.

Setup HTTP

The Internet Services HTTP screen enables the System Administrator to specify the Keep Alive Timeout, Maximum Connections, Port Number and Secure HTTP (SSL) settings.

1. At your Workstation, open the web browser, enter the *IP Address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[HTTP]** in the directory tree.
8. The **[Keep Alive Timeout]** setting determines how long the device's Internet Services pages will wait for a response from a connected user before terminating the connection. Enter the required number of seconds (1 - 60) in the **[Keep Alive Timeout]** entry box.

   Note

   Generally, user connections will be adversely affected (slow or kept busy) if the Keep Alive Timeout is set for a longer period of time.

9. The **[Maximum Connections]** setting is the maximum number of simultaneous connections that can occur at any given moment to Internet Services. Enter a number from 8 - 32 to indicate the maximum number of clients that can be connected (for example, with open sockets) to the HTTP server at any one time in the **[Maximum Connections]** entry box.

   Note

   Before enabling the HTTP Security Mode the device **must** have a Machine Digital Certificate configured. For information on Machine Digital Certificate, see Machine Digital Certificate Management on page 8-9.

10. To set the HTTP Security Mode, select enable for the **[Secure HTTP (SSL)]** option.
11. Change the HTTP **[Port Number]** if required. The default is 80.
12. Click on the **[Apply]** button to accept the changes.

How to verify the IP Address

The device is configured by default to request an IP address from a DHCP server. If your DHCP server provides a valid IP address you will not need to configure the device with an IP address. HTTP is also enabled by default. Print a Configuration Report to verify the IP address.

To print a Configuration Report on demand, go to the device:

1. Press the **<Machine Status>** button on the device.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

How to Add or Change a Static IP Address when there is no DHCP Server Available

At the Device

1. Press the **<Log In/Out>** button.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, then touch **[Enter]**.
3. Touch the **<Machine Status>** button.
4. Touch **[Tools]**.
5. Touch **[Network Settings]**.
6. Touch **[TCP/IP Settings]**.
7. Touch **[Dynamic Addressing]**.
8. Touch **[Disable]** to disable DHCP, and touch **[Save]**.
9. Touch **[IP Address/Host Name]**.
10. Touch **[IP Address]** and enter a valid IP Address and touch **[Save]**.
11. Touch **[Host Name]** and enter host name and touch **[Save]**.
12. Touch **[Close]**.
13. Touch **[Subnet and Gateway]**.
14. Touch **[IP Gateway]** and enter a valid gateway address and touch **[Save]**.
15. Touch **[Subnet Mask]** and enter a valid subnet mask address and touch **[Save]**.
16. Touch **[Close]**.
17. Touch **[TCP/IP Enablement]**, ensure it is enabled and touch **[Save]**.
18. Touch **[Close]**.
19. Press the **<Log In/Out>** button.
20. Touch **[Logout]** to exit the Tools pathway.

Configure Protocols with Internet Services

Internet Services is a series of web pages, hosted on the embedded HTTP server of the device, allowing configuration of services and settings using a web browser.

Refer to the Protocols section of this guide and follow the instructions to configure protocols.

To configure individual protocols only, using your web browser, perform the following steps:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter].**
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link, then click on the **[Protocols]** link.

   Note

   To see IPv6 addressing parameters, if desired, click IP (Internet Protocol) in the list of Protocols, then click on IP (v6).

6. Select your individual protocol of interest from the displayed list and modify settings to your requirements.

Configure additional purchased options

Refer to the Options section of this guide and follow the instructions provided.

Note

If you are installing multiple devices on your network, you may find the Cloning feature useful. This feature enables you to copy a number of configuration settings from one device to another. For more information, see the Cloning topic in this guide.

This device offers enhanced security. For information, refer to the Security and Authentication sections.

Install Printer Drivers

Refer to Print Drivers on page 6-1 of this guide and follow the instructions provided.

General Setup 3

Set a Description for the Device

The CentreWare Internet Services Properties Description page contains information that identifies a specific device model, name and physical location.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Select **[Description]** in the directory tree.
6. Type a name of your choice for the device in **[Device Name]**.
7. Type the site location for the device in **[Location]**.
8. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.

Administrator Tools Password

The Administrator password is required to access the administrator tools function both from the device touch screen and CentreWare Internet Services. Access to the administrator tools is necessary to configure the device, network connectivity and optional settings.

> Note
> Note that the web user interface (Internet Services) is now protected by the Administrator password, so that you will need to log in with the User ID and Password, the default is **admin** and **1111**. BEFORE modifying any settings. After working with settings, make sure to log out by clicking on **[admin-Logout]** in the upper right corner of the Internet Services screen, then click on the **[Logout]** button.

We recommend that you change the Administrator password immediately after device installation. A password of at least 9 characters in length should be sufficient for a year. Once changed, ensure the password is kept in a secure place for future use.

How to change the Administrator Password

New Password

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.

3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Select **[Admin Password]** in the directory tree.
7. Ensure **New Password** tab is highlighted on the top of the screen.
8. Enter detail in the **[New Password]** and **[Retype New Password]** fields.
9. Click on the **[Apply]** button.

Note

The user name **"admin"** is reserved for the Device System Administrator Account.
Do NOT use the username **"admin"** for any local or network accounts on the device.

Configuration Page

The Configuration page allows you to view device setup details, for example Network Setup and Workflow Scanning Setup.

Note

These details can also be printed by clicking on the **[Print Configuration Page]** button.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Select **[Configuration Report]** in the directory tree.
4. To view information about a setting select the required configuration setting from the list.
5. To print the Configuration details, click on the **[Print Configuration Page]** button.

How to Print a Configuration Report

The Configuration Report details the device software versions and network settings configured for the device. The Configuration Report automatically prints when the device is rebooted or powered on. You can print a Configuration Report by following the instructions below.

At the Device

1. Press the **<Machine Status>** button on the device.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

How to Disable the Configuration Report from Printing at Power On

At the Device

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.

4. Touch **[Device Settings]**.
5. Touch **[Configuration/Information Pages]**.
6. Touch the **[No]** button under **Print Configuration at Power On**.
7. Touch **[Save]**.
8. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

Configure Print Protocols

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. At the welcome page, click on the **[Configure Device]** button.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. If you want to use the checklist, click on the **[View Checklist]** button and click on the **[Print]** button. Scroll to the bottom of the screen and click on the **[Close]** button.
6. Click on the **[Settings]** button next to **Print Protocols**.
7. Click on the **[Configure]** button next to **General Settings** to configure general print settings.
8. Click on the **[Save]** button when you have finished configuring general settings.
9. Click on the **[Configure]** button next to the **IP (Internet Protocol),** to enable on the device to support your network environment.
10. Enter the information for your chosen protocol. If you need more information on how to configure protocol information refer to Network Installation on page 5-1.
11. Click on the **[Save]** button. You have finished configuring the protocol information, click on the **[Close]** button.
12. To print to the device, install the printer drivers on your workstation. If you need more information refer to Print Drivers on page 6-1.

Configure Services

If you have installed one or more optional service on your device you can configure the service from Internet Services.

If you need more specific information about services and how to configure them, refer to the following chapters for each service:

- Workflow Scanning on page 10-1
- E-mail on page 13-1
- Internet Fax on page 14-1
- Server Fax on page 23-1
- Embedded Fax on page 15-1
- LAN Fax on page 16-1
- Network Accounting on page 20-1

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.

5. Select **[Configuration Overview]** in the directory tree.
6. Click on the **[Settings]** button next to the service that you want to configure, for example E-mail.

   Note

   If you cannot see any services, then they have not been installed on your device.

7. Click the **[Configure]** button next to each step and enter the information to configure your service. Click on the **[Save]** button when you have finished with each screen.
8. If you have more than one service to configure, click on the **[Configure Next Service]** button. Otherwise, click **[Close]**.
9. Test your service at the device to verify that it is configured correctly.

Cloning

Cloning enables you to copy the settings and web generated scan templates of one device and transfer them to other devices operating with the same version of system software. Depending on the optional features installed on the device, groups of settings can be cloned. For example, scan settings will be available for cloning only if the Workflow Scanning optional feature is already installed on the source device.

After selecting the settings to be cloned, a configuration cloning file is created and saved with the extension .dlm (downloadable module).

The configuration cloning file can then be submitted to other devices using Internet Services via a web browser. The settings are transferred and applied to the recipient device.

Note

Optional features must be installed on the recipient device in order to accept cloned settings. In other words, it is not possible to install an optional feature (for example, Workflow Scanning or E-mail) through the process of cloning.

All devices involved in the cloning procedure must contain the same system software version.

To Verify the Software Version

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Configuration]** in the directory tree.
7. Scroll down to the **Software Versions** area and view the System Software version.

To Clone a Device

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.

4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Cloning]** in the directory tree.
7. From the **Create Clone File** area, check to boxes next to the feature to select the settings that you wish to clone. To clone all features, click on the **[Select All]** button, or to customize the configuration file disable any of the features by clicking the checkboxes next to the feature(s) and then click on the **[Clone]** button.
8. In the **Cloning Instructions** area, right-click on the **["Cloning.dlm"]** link that appears and select **[Save Target As]**.
9. A dialog box will prompt you to specify a name and location for the cloned file. Ensure the extension reads **'.dlm'**.
10. Click **[Save]**. The '.dlm' file can now be used to clone other devices.

To Install the Clone File on Another Device

Note

This procedure will cause the device to reboot and will be unavailable over the network for several minutes.

1. Click on the **[Status]** tab.
2. Select **[Welcome]** in the directory tree.
3. Click on the **[I Have A Cloning File]** button.
4. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
5. Click on the **[Login]** button.
6. Scroll down to the **Install Clone File** area, click on the **[Browse]** button to locate your file.
7. Click on the **[Open]** button, then click on the **[Install]** button.

The device will be unavailable over the network for several minutes. Once rebooted a Configuration Report will print, if enabled.

Image Settings

The Image Settings screen allows you to set preferences for the various file formats that the device is capable of creating when features such as E-mail and Internet Fax are used at the device.

Accessing Image Settings (including Linearized PDF) and XPS

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Image Settings]** in the directory tree.
7. Select and configure the Image Settings for the various file formats as desired.
8. When done, click on the **[Apply]** button.

9. Click on the **[OK]** button, when you see a dialog box that says **"Properties have been successfully modified"**.

TIFF (Tagged Image File Format) Settings

Tagged Image File Format is a multi-platform format for raster (bitmapped) graphics. Nearly every graphics application can read and write TIFF. Depending upon your needs, select which version of TIFF Compression the device will use.

- TIFF 6.0 (old JPEG)
- TIFF Specification Supplement 2 (new JPEG).
- LZW - This is a lossless compression method yielding very high compression efficiency, LZW works best for files containing repetitive data, such as is the case with text and monochrome images. LZW has long been associated with TIFF and GIF images. This compression algorithm was widely used in Adobe Photoshop, until version 6, and Adobe Acrobat, until version 5.

PDF & PDF/A Settings

Select Optimized for Fast Web Viewing if you want to create linearized PDF files. Linearized PDF files allow the first page of the PDF file to be displayed in a user's web browser, before the entire file is downloaded from the web server. This fast first page display helps to alleviate Internet user frustration in waiting for an entire file to download before displaying the file's contents.

Select MRC Compression if you want to use Mixed Raster Content (MRC) compression. MRC is used to divide the scanned image based on content, and then compress each area in the optimal manner for that image area. This option allows for smaller output files with better image quality.

Note

Regarding Searchable PDF and PDF/A: If this option is available, by enabling the selection you will provide Workflow Scanning, E-mail, and Internet Fax users with the ability to choose [Searchable] as an option for their PDF and PDF/A file formats. The Searchable Format provides a second layer of data with the text of the scanned document. The second layer is converted to an optical character readable format, enabling the text of the document to be searched on, copied, and pasted, as desired.

JBIG2

JBIG is a standard algorithm for lossless compression of bi-level images (two color images), specializing in the preservation of thin lines. JBIG2 compression is usually used for text and halftone documents, and is claimed to be able to compress scanned documents up to 10 times smaller than with TIFF G4. A further claim is that it allows scanned manuals, books, check images, and other document types to be viewed and manipulated efficiently over the Internet. This method yields a very small black and white file size with fast viewing performance. This compression format requires Acrobat 5, with PDF version 1.4 or greater.

Flate Compression

Select Enabled or Disabled. Flate is a lossless compression algorithm based on two other algorithms: Huffman compression and LZ77 (the first LZW). Huffman compression is a lossless algorithm ideal for compressing text. LZ77 works well with files containing lots of repetitive data, such as text and monochrome image (TIFF and GIF) files. Flate compression is a standard feature of PDF files that Acrobat works well with.

XPS Settings

XPS is Microsoft's new electronic paper format, an alternative to PDF. XPS is currently supported as a saved file format in Microsoft Office 2007, with an XPS viewer built into Windows Vista. Microsoft states that Windows vista uses the XPS format as a document format, a windows spool file format, and a page description language for printers.

Select **[Optimized for Fast Web Viewing]** (also known as Interleaved XPS), or **[Enable MRC Compression]** for the same reasons stated above for PDF files.

Note

Regarding Searchable XPS: If this option is available, by enabling the selection you will provide Workflow Scanning, E-mail, and Internet Fax users with the ability to choose [Searchable] as an option for their XPS file format. The Searchable Format provides a second layer of data with the text of the scanned document. The second layer is converted to an optical character readable format, enabling the text of the document to be searched on, copied, and pasted, as desired.

Accessing Image Settings

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[Default Template]** in the directory tree.
8. Scroll to the **Workflow Scanning** area, click on the **[Edit]** button.
9. Within Workflow Scanning, scroll to the **Original Type** area - select either the **[Photo & Text]**, **[Text]**, **[Map]** or **[Newspaper/Magazine]** radio button.
10. Then select the **[for OCR]** radio button in the **Scan Presets** area.
11. Click on the **[Apply]** button.
12. Scroll to **Filing Options** area, click on the **[Edit]** button.
13. Within Filing Options, for **File Format** - select one of either **[TIFF], [mTIFF], [JPEG], [PDF], [PDF/A]** or **[XPS]** radio button.
14. Scroll down to **Searchable Options** within File Format and select the **[Searchable]** radio button.
15. Click on the **[Apply]** button.
16. Under **Workflow Scanning Image Settings** area, click on the **[Edit]** button.
17. Within **Searchable XPS PDF & PDF/A Defaults** area, under **Searchable Options** select the **[Searchable]** radio button and the correct language for your device.
18. Click on the **[Apply]** button.

At the Device

1. Press the **<Services>** button.
2. Touch the **[Workflow Scanning]** icon.
3. Input documents to scan and touch the **[Start]** button.

Accessing Workflow Scanning, E-mail, or Internet Fax Settings

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on either **[Workflow Scanning]**, **[E-mail]**, or **[Internet Fax]** link.
7. For Workflow Scanning, select **[Default Template]** in the directory tree, then click on the **[Edit]** button within the **Filing Options** area. Select the **[Searchable]** radio button under **Searchable Options**.
8. For E-mail or Internet Fax, select **[Defaults]**, then select the **[Edit]** button within **Filing Options**. Select the **[Searchable]** radio button under **[Searchable Options]** within **Document Format** as the user presented scanning default.
9. When done, click on the **[Apply]** button to save changes or **[Undo]** to remove changes and refresh the page.

Internationalization

The Internet Services Internationalization screen allows administrators to specify the locale where the device is situated. This is used to determine the type of coding used by the device to interpret data, such as print jobs.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Internationalization]** in the directory tree.
7. Specify the locale, select the required setting from the **[Selected Locale]** drop down menu. The device will make an assumption on the encoding that are most likely used.
8. If you want to enter the specific encoding of user strings provided for the device, select **Custom** form the **[Selected Locale]** drop down menu, and select the required encoding priority order.
9. Click on the **[Apply]** button to save your changes.

Job Deletion

The Job Deletion page allows you to set permission that allow System Administrators or non-administrator users to delete jobs from the device print queue.

> Note
> System Administrators can always delete any job, regardless of the setting selected on the Job Management Page.

At the Device

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button.

4. Touch the **[Tools]** tab.
5. Touch **[Security Settings]**.
6. Touch **[Authentication]**.
7. Touch **[Job Deletion]**.
8. Touch either:
   - **[All Users]** to allow any user to delete any job in the job list. There is no authentication needed when the user clicks on a job in the job list and selects **Delete**.
   - **[System Administrators Only]** to allow only users with administrative access (password) to delete jobs. The System Administrator must provide a username and password when deleting a job.
9. Touch **[Save]** button.
10. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

Extensible Service Setup

SMart eSolutions

SMart eSolutions provides a setup page to guide you through the steps required to configure the device for automatic meter readings. SMart eSolutions enables the device to automatically send data to Xerox to be used for billing (Meter Assistant) and solid ink (Supplies Assistant).

There are three ways to register the device for SMart eSolutions:

- Client Direct registration
- SMart eSolutions Windows Client
- CentreWare web

For a full description of SMart eSolutions and to download the applications (SMart eSolutions Windows Client or CentreWare web), refer to: www.xerox.com/smartesolutions.

> Note
> SMart eSolutions is not available in all countries. Refer to your Xerox Representative for further information.

Information Checklist

Before registering the device for Meter Assistant, please ensure the following items are available or have been performed.

- Create an account on Xerox.com. Add all devices in inventory that you wish to register for Automatic Meter Readings to your account.
- Ensure the device is fully functioning on the network.
- TCP/IP and HTTP protocols must be enabled on the device so that the device's web browser can be accessed.
- Enable SNMP (Smart eSolutions Client and CentreWare web). If you want to use Smart eSolutions Windows Client or CentreWare web. Visit www.xerox.com/smartesolutions for further instructions and to download the software.

SMart eSolutions Information

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Select **[SMart eSolutions]** in the directory tree.
4. In the **Enrollment** section, verify that the **[Enrolled]** radio button is selected.
5. The **Communication Setup** section indicates if your device is successfully communicating to Xerox. If there is an error in communication or HTTP Proxy Server is not configured, click on the **[Configure]** button to update the internet proxy settings.
6. In the **HTTP Proxy Server** area, check the **[Enabled]** checkbox.
7. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
8. Enter the *IP Address* settings or the Host Name and click on the **[Save]** button to return to the SMart eSolution Setup page.
9. To change the **Daily Transmission Time** click in the time box and change the time to the required time
10. Click on the **[Apply]** button

Meter Assistant

Verify devices are enabled on Xerox.com

1. Go to www.xerox.com
2. Click on "**Submit Meter Reads**"
3. Login to Xerox.com, and ensure all devices are enabled for automation.

If devices are not enabled, submit for enablement on Xerox.com. Check back on Xerox.com after 24 hours.

Supplies Assistant

Eligible devices will automatically be enabled for Supplies Assistant once the device is registered with Xerox. When you call to order supplies, let the representative know the on-hand balance and that you would like to use Supplies Assistant.

Energy Saver

Allows you to set the device to save energy when not in use.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Energy Saver]** in the directory tree.
7. In the **Energy Saver Mode** area, select one of the following mode:
   - **Intelligent Ready** - wakes up and sleeps automatically based on previous usage.
   - **Job Activated** - wakes up when activity is detected.
   - **Scheduled** - wakes up and sleeps at set times on a daily basis.

8. Select **Fast Resume** to **[On]** to reduce the time taken for the device to wake up.
   This will change the default sleep/low timeout and increase energy usage.
9. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.

Alert Notification

In the Alert Notification section you can set up groups to notify (by e-mail) when problems occur on the device. Alert notification is configured via Internet Services.

To Set up an Alert Notification Group

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Alert Notification]** link.
7. Select **[E-mail Alerts]** in the directory tree.
8. Check the **[Enable Group 1]** box in the **Recipient Group Addresses** area.
9. Click the filed under **E-mail Addresses**, and enter an e-mail address or addresses.
10. Enter an e-mail address in the **["Reply To": E-mail Address]** box.
11. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
    The **"Settings confirmed. Send a test e-mail?**" window will appear. Click on the **[OK]** button if you wish to send a test e-mail to the Alert Notification recipient(s), or **[Cancel]** to return to the Alert Notification page.

To Assign Notification Alerts to a Group

12. Scroll down to the **Recipient Group Preferences** area. Select the Status Codes that you wish the group(s) to be notified of by checking the appropriate boxes. Click the **[Glossary]** link next to Status Codes in the **Recipient Group Preferences** area for further information about the Status Codes.
13. Enter the number of minutes for the **[Set Jam Timer for release of status to selected groups]** (0-60 minutes).
14. Click on the **[Apply]** button to save your settings.
15. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

To Edit or Delete a Recipient Address

1. Select the address from the Group list and click on the **[Edit]** button.
2. Select either:
   - **To edit**: make the required changes and click on the **[Replace]** button.
   - **To delete**: select an address from the Group list, click on the **[Delete]** button.

3. When you have finished making changes click on the **[Apply]** button to save or **[Undo]** to cancel. The **"Settings confirmed. Send test e-mail?"** window will appear. Click on the **[OK]** button if you wish to send a test e-mail to the Alert Notification recipient(s), or **[Cancel]** to return to the Alert Notification page.

Billing Meter Read Alerts

Using this dialog, System Administrators can set up an e-mail notification to the designated Billing Administrator whenever billing meters are automatically read by the Meter Assistant.

To Set up a Billing Meter Read Alert

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Alert Notification]** link.
7. Select **[E-mail Alerts]** in the directory tree.
8. Check the box labelled **[Billing meter reads reported]** under **Recipient Group Preferences** area
9. Click on the **[Apply]** button.
10. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

Local UI Alerts

System Administrators can set up the local UI (user interface) to warn users that the scan disk is running low on memory, potentially impacting system performance and/or causing job loss.

To Set up the Local UI Alert

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Alert Notification]** link.
7. Select **[Local UI Alerts]** in the directory tree.
8. Select the radio button corresponding to the warning that you wish to provide, if **[Custom]** is selected, enter an amount between 0 - 75 in the **[Custom]** box.
9. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
10. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

Billing Information and Usage Counters

The Billing and Counters page provides the Billing information for the device, including number of impressions printed or copied.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Select **[Billing Information]** in the directory tree to view Current Billing information. and click on the **[Refresh]** button to refresh Billing information.
4. Select **[Usage Counters]** in the directory tree to view the counts from the Usage Counters; click on the **[Refresh]** button to refresh the Usage Counters.

Banner Sheet

When documents are sent to print at the device, a banner sheet is printed identifying the PC that sent the print job. It is possible to disable this setting both within the printer driver and from the device administrator tools. These instructions describe how to disable the banner sheet from the device.

At the device

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch **[Job Sheets]**.
6. Touch **[Banner Sheets]**.
7. Touch the **[Disabled]** button.
8. Touch **[Save]**.
9. Press the **<Log In/Out>** button, then press **[Logout]** to exit the Tools pathway.

Saving and Reprinting Jobs

The Save Job for Reprint feature allows users to store print jobs on the device from their print driver, or the Print page of Internet Services, then select the job from the device's user interface for reprinting.

This feature can be enabled and configured by the System Administrator from the Properties page of Internet Services (the series of web pages, hosted on the embedded HTTP server of the device).

Enabling the feature at a TCP/IP Networked Workstation

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. if prompted, enter the administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.

5. Click on the **[Reprint Saved Jobs]** link.
6. Select **[Enablement]** in the directory tree.
7. Click the **[Enabled]** radio button to enable the feature, and click on the **[Apply]** button.

Backup Saved Jobs

1. Select **[Backup Jobs]** in the directory tree to back up saved jobs stored on the system.
2. Under Settings, from the **[Protocol]** drop-down menu, note that only FTP is available.
3. Select either the **[IP Address]** or **[Host Name]** radio button for your FTP server.
4. Specify the *IP address* or *host name* of the repository.
5. For **[Document Path]**, specify the path to the file repository.
6. For **[File Name]**, type the file name for the backup. This name will be appended onto the end of the document path.
7. For **[Login Name]**, if you selected System for Login Credentials (referring to FTP repository in the Workflow Scanning topic), then you must specify the system login name here.
8. For **[Password]** and **[Retype Password]**, if you selected System for the login credentials, then you can specify and confirm the system password here. The password may be blank.
9. Check **[Select to Save New Password]** for an existing Login Name. You must then click the **[Start]** button at the bottom of the page to implement the password change, or **[Undo]** to cancel any changes.

Restore Saved Jobs

1. Select **[Restore Jobs]** in the directory tree to restore saved jobs stored on a repository.

   Note

   When Saved Jobs are restored, all current Saved Jobs data will be immediately deleted. The restore process may take considerable time to complete depending on how many files were backed up. The restored Saved Jobs data is not appended to the existing Saved Jobs If the restore is aborted, the Default Public Folder will be empty.

2. Note that only FTP is available in the **[Protocol]** drop-down menu under Settings.
3. Select either the **[IP Address]** or **[Host Name]** radio button for your FTP server.
4. Specify the IP address or host name of the repository.
5. For **[Document Path]**, specify the path to the file repository.
6. For **[File Name]**, type the file name for the backup to restore. This name will be appended to the document path.
7. For **[Login Name]**, if you selected System for Login Credentials (referring to FTP repository in the Workflow Scanning topic), then you must specify the system login name here.
8. For **[Password]** and **[Retype Password]**, if you selected System for the login credentials, then you can specify and confirm the system password here. The password may be blank.
9. Click **[Select to Save New Password]** for an existing Login Name. You must then click on the **[Start]** button at the bottom of the page to implement the password change, or **[Undo]** to cancel any changes.

Online / Offline

The Online/Offline window allows the System Administrator to stop and resume the system from receiving or sending jobs over the network.

At the device

1. Press the **<Log In/Out>** button to enter the Tools pathway.

2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch the **[Tools]** tab.
5. Touch **[Network Settings]**.
6. Touch **[Online/Offline]**.
7. To stop the device receiving or sending jobs over the network touch the **[Offline]** button. Any installed optional features using the network (for example Workflow Scanning) will not be available until the device is set to Online.

   Note

   To enable the device to receive or send jobs over the network touch the **[Online]** button.

8. Touch **[Close]**.
9. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

Auxiliary (Foreign Device) Interface Kit

A third party access and accounting device, such as a coin operated device or a card reader can be attached to the device. To enable this option, the Foreign Device Interface Kit must be installed. After the kit is installed the administrator must enable Auxiliary Access as the Accounting Mode from the Tools menu of the device, as follows:

1. Press the **<Log In/Out>** button.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch the **[Tools]** tab.
5. Touch **[Accounting Settings]**.
6. Touch **[Accounting Mode]**.
7. Select **[Auxiliary Access]** and select available buttons to configure your device.
8. Once selected, touch **[Save]**.
9. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

For further instructions on Auxiliary (Foreign Device) Interface Setup options refer to the **Interactive User Guide** delivered with your device.

SNMP (Simple Network Management Protocol)

It is possible to remotely define and modify GET, SET, and TRAP SNMP (Simple Network Management Protocol) community names for the device. You can also configure SNMP trap destinations for TCP/IP and NetWare (IPX) that will receive traps from any device on the network.

SNMP Community Name properties that can be configured are:

- GET Returns the password for SNMP GET requests to the device. Applications obtaining information from the device via SNMP, such as Xerox PrinterMap or CentreWare, use this password.
- SET Returns the password for SNMP SET requests to the device. Applications that set information on the device via SNMP, such as Xerox PrinterMap or CentreWare, use this password.
- TRAP Returns the password for SNMP TRAPS from the device. This is the default password for SNMP TRAPS sent from the device via SNMP.

Configure SNMP Community Names

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** button.
6. Click on the **[Protocols]** link.
7. Select **[SNMP]** in the directory tree.
8. Check the **[Enable SNMP v1/v2c Protocol]** or **[Enable SNMP v3 Protocol]** box to enable the protocol.
9. To edit SNMP properties click either **[Edit SNMP v1/v2c Properties]** or **[Edit SNMP v3 Properties]**.

   Note

   Configure **HTTPS** before editing SNMP v3 Properties. Configuring this feature requires secure web page communication.

   Turning off the SNMP protocols will cause an interruption in the communication between the device and remote client applications.

10. Enter a name (up to 256 characters) for the **[GET Community Name]**. The default is **public**.
11. Enter a name (up to 256 characters) for the **[SET Community Name]**. The default is **private**.

CAUTION

If you change the GET and/or SET Community Names, you must change all network applications that are communicating via SNMP with this device to use the new GET/SET names.

12. Enter a name (up to 256 characters) for the default **[TRAP Community Name]**. The default is **SNMP_trap**. The Default TRAP community name is used to specify the default community name for all traps generated by this device.
13. Click **[Save]**, to apply the changes or **[Undo]** to return to the previous settings.
14. In the **Authentication Failure Generic Traps** area, check the **[Enabled]** box if you want the machine to generate a trap for every SNMP request that is received by the machine which contains an invalid community name.
15. Click on the **[Apply]** button to accept the changes or **[Undo]** return to the previous settings.

Software Upgrade via Network Connection

WARNING
This procedure will delete any current jobs in the device print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software. All configured network settings and installed options will be retained by the device after the Software Upgrade process.

Prepare for the Upgrade

Obtain the new software upgrade file for your device from the www.xerox.com website or from your Xerox Customer Support Representative. Download the upgrade file to a local or network drive. You will be able to delete the file after the upgrade procedure.

It is important to obtain the correct upgrade file for your device. Determine the software version you are currently running, as follows.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Configuration Report]** in the directory tree, scroll down to the **Common User Data** section to see your System Software Version.

Upgrades

The Software Upgrade feature allows the customers to upgrade the device software as requested by a Xerox Customer Support Center Representative, without needing a Customer Service Representative to be present.

To enable or disable software upgrades on the device, follow the procedure below:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Select **[Upgrades]** in the directory tree.
8. In the **Upgrades** area, check the **[Enabled]** box to enable Machine Software upgrade.
9. Click on the **[Apply]** button.

Manual Upgrade

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Select **[Manual Upgrade]** in the directory tree.

   Note

   Note the current software level in the Last Successful Upgrade box.

8. In the Manual Upgrade box select **[Browse]** to locate the software upgrade file obtained earlier.
9. Select the file and click **[Open]**.
10. Click on the **[Install Software]** button to proceed with the upgrade. The file will be sent to the printer and will disable the printing functionality. The web browser will become inactive and you will not be able to access the device via this method until the upgrade has completed and the device has rebooted. The upgrade should take no longer than 15 minutes.
11. Once the device has completed the upgrade it will reboot automatically. The configuration report will print (if it was enabled in the Tools set up). When the device is accessible from a web browser, view the software version on Internet Services Manual Upgrade page, or check the configuration report to verify that the software level has changed.

    Note

    Your device can be set to automatically schedule device software upgrades from a central server at a specific time on a regular basis. For instructions click the Software Upgrade link to the left of the page and select Auto.

You have completed the steps to perform a manual software upgrade.

Software Upgrade: Auto

Your device can be set to automatically schedule device software upgrades from a central server.

WARNING
This procedure will delete any current jobs in the device print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software. All configured network settings and installed options will be retained by the device after the Software Upgrade process.

Before You Start

Determine your current System Software Version number.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.

4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Configuration Report]** in the directory tree, scroll down to the **Common User Data** section to see your System Software Version.
7. Contact your Xerox Customer Support Representative to make certain that Auto Upgrading is appropriate for your device. If it is not, refer to the Software Upgrade via Network Connection topic for manual upgrade instructions.
8. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

Set the Auto Upgrade Time

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Select **[Auto Upgrade]** in the directory tree.
8. Check the **[Enabled]** box to enable the Auto Upgrade feature.
9. Select either **[Hourly]** or **[Daily]** to activate the feature accordingly, in the **Refresh Start Time** section.
10. If **[Daily]** has been selected, enter the required time for the upgrade to be performed.
11. If IP Address is selected, enter the IP address of the server where the software upgrade file (obtained earlier) is located, in the **[File Server IP Address]** field and if Host Name is selected, enter the Host Name in the **[Host Name]** field.
12. Enter the path to the upgrade file on the server in the **[Directory Path]** field.
13. Enter the **[Login Name]** and **[Password]** for the server, retype the password.
14. Click on the **[Apply]** button to accept the changes.

The upgrade will now be performed automatically on the device at the time specified. Once the upgrade process starts network connectivity with the device will be unavailable, including access from Internet Services. The upgrade progress can be monitored from the device screen interface.

You have completed the steps to automatically upgrade the device software.

4 CentreWare Internet Services

This chapter explains how to enable and use the Internet Services feature of the device.

The Internet Services feature uses the embedded HTTP Server on the device. This allows you to communicate with the device through a web browser and gives you access to the Internet or intranet. Entering the IP Address of the device as the URL (Universal Resource Locator) in the browser provides direct access to the device.

Internet Services not only allow you to change basic settings as in the Control Panel, but also allows you to change more specialized settings for the device.

Information Checklist

Before accessing Internet Services, please ensure the following items are available or have been performed:

- The device must be physically connected to the network with TCP/IP enabled so that Internet Services can be accessed from a web browser.
- An existing operational workstation with TCP/IP Internet or Intranet accessibility is required.
- HTTP (HyperText Transfer Protocol) should be enabled on the device. HTTP is enabled by default. If you need to enable HTTP, see Enable HTTP on the device on page 4-1.

Enable HTTP on the device

HyperText Transfer Protocol (HTTP) must be enabled on the device in order to access the embedded HTTP server.

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press **<Machine Status>**, then touch the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[Advanced Settings]**.
6. Touch **[Continue]**.
7. Touch **[HTTP Settings]**.
8. Touch **[Enable]**.
9. Touch **[Save]**.
10. Touch **[Close]**.
11. Press the **<Log In/Out>** button, touch **[Logout]** to exit the Tools Pathway.

Access Internet Services

Instructions to access Internet Services:

1. Open the web browser from your Workstation.
2. In the URL field, enter http:// followed by the IP Address of the device. For example: If the *IP Address* is *192.168.100.100*, enter the following into the URL field: *http://192.168.100.100*.
3. Press **[Enter]** to view the Home page.
4. Click a tab to access the desired page, or click on the Index icon at the top of the device web page to access the index and contents list.

Many of the features available within Internet Services will require the **System Administrator Login ID** and **Passcode**. The default being **[admin]** and **[1111]**. A user will only be prompted for the Administrator User ID and Password once in a single browser session.

Status

Description and Alerts

The Description and Alerts page allows you to view the Device Model, Name, location, IP Address and Status of the device.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Click on the **[Description and Alerts]** link.

Alerts

The Alerts page allows you to view all current alert messages. Each alert will specify what the problem is and a solution to the problem.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Click on the **[Description & Alerts]** in the directory tree.

The following information is displayed in the **Alerts** field:

- **Severity** - The importance or impact of the problem.
- **Status Code** - If the problem needs a Service Representative to fix it then let them know this code when you talk to them.
- **Description** - Displays a warning or the problem and how to fix it.
- **Skill Level** - Displays the suggested skill level needed to fix this problem. The levels are:
  - **Trained** - System Administrator needed to fix this problem
  - **Untrained** - Normal user can fix this problem
  - **Field Service** - Xerox Support needed to fix this problem

- **Management** - Network Administrator needed to fix this problem
- **No intervention required** - A normal device status.

Rebooting the device

It is possible to reboot the device from Internet Services.

1. Click on the **[Status]** tab.
2. Click on the **[Description & Alerts]** in the directory tree.
3. Click on the **[Reboot Machine]** button and click **[OK]** to reboot the device. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

Billing Information and Usage Counters

The Internet Services Billing Information page displays the total number of impressions copied, printed, scanned or faxed by the device. The Usage Counters page shows you the number of impressions and images sent by the device.

Billing Information

The Billing Information page provides current and previous readings of all device counters.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Click on the **[Billing Information]** in the directory tree.
4. Click on the **[Refresh]** button to view the current billing information in the Total Impressions area.

Usage Counters

The Billing Meter area shows the date and number of impressions that were notified to the Xerox Communication Server, if this has been set up.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Click on the **[Usage Counters]** link.
4. Click on the **[Refresh]** button to view the current usage in the Usage Counters area.

Consumables

The Consumables page allows you to view the status of the Customer Replaceable Units (CRUs) within the device.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Click on the **[Consumables]** in the directory tree.

4. The **[Consumables]** screen will show consumable information for:
   - **ColorQube Stick**
   - **Cleaning Unit**
   - **Document Feeder Feed Roller**

   The Status will display either one of the following:
   - **OK**
   - **Reorder** (Supply is getting low)
   - **Replace** (Unit Supply is used up and requires immediate replacement).

For each unit, the **[Life Remaining]** icon describes the current supply level as a percentage and provides a bar graph visual display.

Trays

The Trays page allows you to view paper supply setup and paper output.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Status]** tab.
3. Click on the **[Trays]** in the directory tree.
4. The **[Trays]** page displays the current paper supply.

Instructions for changing the paper stock are contained in the **Interactive User Guide** delivered with your device.

Jobs

The **[Jobs]** tab displays a list of active and completed jobs. You can also delete jobs in this tab.

Note

The details displayed may differ from those shown on the device's touch screen.

Active Jobs

The Active Jobs page displays information about the active job list on the device:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Jobs]** tab, **[Active Jobs]** will display.
3. Click on the **[Refresh]** button to update the information in the table.
   The following information is shown:
   - **Job Name** - The title of the print job
   - **Owner** - The person submitting the job
   - **Status** - The current status of the job
   - **Type** - Displays whether the job is print, scan or fax
   - **Copy Count** - Displays the number of copies requested for the job

Saved Jobs

Within the **Jobs** tab screen select the **[Saved Jobs]** tab.

The screen will display the Saved Jobs, the memory used on the device, you can also create new saved job folders and manage saved job folders.

Print

Print-ready documents can be quickly and easily submitted for printing using the Job Submission page.

A print-ready document is a file that has been formatted and saved for printing from the source application or the Print to File check box was selected in the printer driver.

The following file formats can be printed from the Job Submission page:

- PCL® 5e
- PCL® XL
- PostScript® Level 2 and 3
- TIFF
- ASCII Text
- PDF
- JPEG

  Note
  ASCII text files, from systems other than PCs, may not print correctly if hard carriage returns (ASCII Control-M) are not used as line delimiters in the text.

Large print jobs need adequate space on your hard drive when printing through Internet Services.

1. At your Workstation, open the web browser from your Workstation. Enter the *IP address* of the device in the Address bar. Click on **[Enter]**.
2. Click on the **[Print]** tab.
3. In the **[File Name]** area at the bottom of the screen, enter the name of the document that you want to print, or click the **[Browse]** to locate the document on your workstation.
4. In the **[Printing]** area, enter the number of **[Copies]** required (between 1 - 9999).
5. Select the required **[Job Type]**:
   - **Normal Print**
   - **Secure Print** - you will need to enter a 4 - 10 digit number which you will use at the device's user interface to release the document for printing
   - **Sample Set**- if several copies of the document have been selected, one copy only will print to allow the reader to check for errors. Once validated, the remaining copies can be released from the device's user interface
   - **Save Job for Reprint** - the document will be saved for reprinting.
   - **Delayed Print** - specify a time for your document to print
6. Select the required Printing options for 2 Sided Printing, Output Color, Collate, Orientation, Staple and Output Destination.

If Network Accounting is installed, then enter your Account and User ID for accounting purposes. (The Accounting fields are only visible if accounting is enabled on your device).

Note

Printing options are only valid for jobs that do not contain the settings already.

7. When finished with your selections, click on the **[Submit Job]** button to send your document to the printer. Wait for the Job Submission confirmation window to appear before exiting or navigating to a different screen, so your print job will not be deleted.
8. Retrieve the printed document(s) from the device.

Properties

This tab allows you to view and set the device properties. These include the device details and configuration, Internet Services settings, the port settings, protocol settings, emulation settings, and the memory settings. The items displayed will depend on the model and configuration of the device.

Configuration Overview

This page displays the device configuration overview, displays information on Connectivity and Printing, if Services are configured or not, if Cloning is configured or not.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Configuration Overview]** link.

Description

This page displays the following information and allows you to set and view information related to the device, such as the name and installation location of the device:

- **Machine Model**
- **Product Code/Serial Number**
- **Device Name**
- **Location**

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Description]** link.
6. If **[Device Name]** and **[Location]** are changed, click on the **[Apply]** button, to accept the changes.

General Setup

Configuration

The Configuration page displays the following information:

- Report Profile
- Common User Data
- Machine Profile
- Machine Hardware
- General Setup
- Software Versions
- Connectivity Physical Connections
- Connectivity Protocols
- Services
- Accounting
- Security
- Media Trays

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Configuration Report]** link from the directory tree.

You can also print a configuration report from this page.

1. To print a configuration report, press the **[Print Configuration Report]** button.

Cloning

This feature, provided by Xerox Standard Accounting, saves the settings of selected features in a configuration file, which can then be used to clone the settings onto other devices. To install configuration files to other devices, the devices must have the same version of software as this device.

The Clone feature will create a **.dlm** file script that can be used to configure other devices. All devices must have the same version of software for the **.dlm** file to be accepted.

The software version is located on the Properties tab, under **General Setup**: **Configuration Report**.

To create a clone file:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Cloning]** link from the directory tree.

7. To clone all features simply click on the **[Select All]** button, or to customize individually, click on the **[Clear All]** button and click to check the individual feature box to be cloned.
8. Click on the **[Clone]** button. The cloning file will be saved as **Cloning.dlm**.
9. To rename file extension, right click on link, select **[Save Target As]**, rename file and click on the **[Save]** button.

To Install a Clone file:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Cloning]** link from the directory tree.
7. Scroll down to the **Install Clone File** area, click on the **[Browse]** button.
8. Select the cloning file, and click on the **[Open]** button.
9. Click on the **[Install]** button.

Note

Once installation of the clone file begins, all internet services from this device will be lost, including the web user interface.
The installation progress can be monitored from the device's interface.

Image Settings

The Image Settings screen allows you to set preferences for compression. The options selected in the Image Settings screen impact the transmission time and size of documents that are created when the E-mail features are used at the device. Settings also impact the job processing time of images scanned with the Workflow Scanning feature.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Image Settings]** in the directory tree.
7. Select the required option for **TIFF Color Compression**. The default is TIFF 6.0 (old JPEG).

Note

Some applications cannot read the default TIFF output. If this functionality is required, click on **[LZW]**. LZW is a lossless general purpose compression, used for color and grayscale TIFF images. LZW creates a larger file size than the other two options that use JPEG compression.

8. For **PDF & PDF/A Settings**, check the enable box for **[Optimized for Fast Web Viewing]** if you want to create linearized PDF files.
   - Linearized files allow single pages of a PDF file to be displayed in a web browser before the entire file is downloaded. This function is recommended if your user create large PDFs which are designed to be delivered to web browsers over the Internet.
   - Large PDF files include those with several pages or contains lots of text and graphics. You can also select Optimized for Fast Web Viewing if users scan to a document management system. This option will reduce the time users have to wait to view PDF files downloaded from the document management system.

     Note

     If you enable Optimized for Fast Web Viewing here it will automatically enable the Optimized for Fast Web Viewing option in both E-mail and Internet Fax Default Image Settings screens.

9. For **JBIG2**, check the enable box option(s) for **[Arithmetic Encoding]** and/or **[Huffman Encoding]** if you want to use JBIG2 compression. JBIG2 is used for monochrome images and/or text within MRC images. JBIG2 will compress text smaller than Group 4 (G4) compression although it takes longer to process. JBIG2 exports PDF files as version 1.4 PDF.
10. Check the enable box for **[Flate Compression],** if you want to add additional lossless compression to any JPEG compression performed by the device.
11. Check the enable box for **[MRC Compression Format (Mixed Raster Content)]** if you want to use MRC compression to create PDF or PDF/A files. MRC is used to divide the scanned image based on content and then compress each area in the optimal manner for that image area. This option allows for smaller output files with better image quality.

    Note

    PDF files are exported as version 1.3 unless JBIG2 is enabled in which case they are exported as 1.4. The use of MRC or Flate do not require 1.4.

12. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
13. Click on the **[Login]** button.

Internationalization

Internationalization allows administrators to specify the locale where the device is situated. This is used to determine the type of coding used by the device to interpret data, such as print jobs.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Internationalization]** in the directory tree.
7. If you want to specify the locale, select the required setting from the **[Select Locale]** drop-down menu. The device will make an assumption on the encoding that are most likely used.
8. If you want to enter the specific encoding of user strings provided for the device, select **[Custom]** from the **[Select Locale]** drop-down menu, and select the required encoding priority order.
9. Click on the **[Apply]** button to save your changes.

Extensible Service Setup

Extensible Service Setup utilizes web based services to enable users to access services. Extensible Service Setup enables independent software vendors and partners to develop customized programs to access directly from the device. Users can enter their User ID at the device and access a set of features and options designed specifically for their business needs.

Note

Before Extensible Service Setup is enabled, **[HTTP (SSL)]** and **[Extensible Service Registration)** must be configured.

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Extensible Service Setup]** link in the directory tree.
7. Check the **[Export password to Extensible Browser]** box to select the required feature in the **Enable Custom Services** area.
8. In the **Browser Settings** area, check to select either or both options **[Enable the Extensible Services Browser]** and/or **[Verify server certificates]** box.
9. Click the **[Apply]** button.

Alert Notification

Customers can set the Xerox device to notify users or operators of problems as they occur on the device. Alert Notification is configured via CentreWare Internet Services.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Alert Notification]** link.

E-mail Alerts

a. Click on the **[E-mail Alerts]** in the directory tree.
b. In the **[Recipient Group Addresses]** area, check the required Group.
c. Click the field under **E-mail Addresses**, and enter e-mail address or addresses.
d. Continue to add e-mail addresses to create your Alert Notification group, as required.
e. In the **[Reply to E-mail Address]** box, enter the address of the administrator or user who is designated to receive any reply e-mails that are sent by users who are listed in the Alert Notification group.

Note

This is normally set to the System Administrator's e-mail address.

f. Click on **[Apply]** to save the changes.

g. If prompted, enter the *User ID* and *Password* of the Administrator's account and click on **[Login]**.

h. The **Settings Confirmed. Send Test e-mail?** window will appear. Click **[OK]** if you wish to send a test e-mail to the Alert Notification recipient(s), or **[Cancel]** to return to the Alert Notification page.

i. If you want to create more than one Alert Notification group, select the group number and add e-mail addresses to the group.

To Assign Notification Alerts to a Group

a. Scroll down to the **Recipient Group Preferences** area. By default, a group will be notified of all device alerts. If you want to select specific alerts, select the alerts that you want Group 1 to be notified of.

b. Click the **Glossary** link next to **Status Codes** in the **Recipient Group Preferences** area for further information about the Status Codes, as below:

- **Machine is stopped:** device has stopped all functions or has been turned off.
- **Potential persistent problems exist:** If area specified does not receive attention problems may re-occur.
- **Machine requires administrator assistance:** Authorized System Administrator must address problem.
- **Machine is operational, but degraded:** device is running at reduced efficiency, needs immediate attention.
- **Paper supply is low:** Paper is running low or wrong size is allocated.
- **Supplies or CRUs are low:** CRU/Solid Ink Sticks or other usable item needs attention (see LUI).
- **Paper jam is detected:** Paper jam is in need of attention in specified area if you have been notified.

c. If you have created more than one group, repeat this exercise for each group.

d. Enter the number of seconds that you want to set the jam timer for release of status to selected groups.

e. Select **[Apply]** to save your settings or **[Undo]** to cancel.

Local UI Alerts

You can configure the device to display a notice on the user interface screen when the scan disk memory is low. The scan disk memory decreases according to the number of pages scanned with the Workflow Scanning, Internet Fax, E-mail or Server Fax features (when these features are installed on the device).

When the scan disk memory is low, scan jobs may slow down or the device may cancel the job.

When a user attempts to scan more pages than the Scan Job Memory Notification setting, the device will display a message to show how many pages can be scanned before the device will slow down or be forced to cancel the job. The default is **30 scanned pages**.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Alert Notification]** link.
7. Click on the **[Local UI Alerts]** In the directory tree.
8. Select the option you want to configure for the number of scanned pages. If you want to specify a number between 1 - 75 scanned pages, select **[Custom]** and enter the number of pages in the box.
9. Click on the **[Apply]** button.

Low Supply Warning

This feature allows you to set the device to display a 'low warning message' about a Supply's level.

By setting a value to '0', the user will see **"NO WARNING MESSAGE"** that the Supply is getting low.

1. Click on the **[Low Supply Warning]** In the directory tree.
2. Select the days remaining from each supply drop-down menu.
3. Click on the **[Apply]** button.

Support

The CentreWare Internet Services Support page provides easy access to the Xerox website. The page can also be set up to show Xerox support telephone numbers and the contact details for the System Administrator.

To Edit Xerox or Administrator Support Contact Details.

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Support]** tab.
3. Click on the **[Edit Settings]** link.
4. Enter the contact details in the entry fields.
5. Click on the:
   a. **[Save]** button to accept the settings If prompted, enter the *User ID* and *Password* of the Administrator's account and click on **[Login]**.
   b. **[Undo]** button to revert back to previous details
   c. **[Cancel]** button to cancel the changes.

Other features and Services

Other features and service that can be configured and is supported by Internet Services are explained throughout this guide.

5 Network Installation

This chapter explains how to set up the device to operate in different network environments.

TCP/IP Settings

This section explains how to set up the device to operate in a Windows TCP/IP environment. The following information is provided:

The device supports IP versions 4 and 6. IPv6 can be used instead of or in addition to IPv4.

IPv4 Settings can be configured directly at the device user interface, or remotely, via a web browser using Internet Services. IPv6 can only be configured using Internet Services. To configure TCP/IP Settings using Internet Services, see Configure TCP/IP Settings using Internet Services on page 5-5.

Configure Static Addressing using the Device

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Existing operational network utilizing the TCP/IP protocol.
- Ensure that the device is connected to the network.
- Static IP Address for the device.
- Subnet Mask Address for the device.
- Gateway Address for the device.
- Host Name for the device.

Enter a Static IP Address

1. At the device and press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, and then the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[TCP/IP Settings]**.
6. Touch **[TCP/IP Enablement]**.
7. Touch **[Enable]** for **IPv4** and **IPv6**.

8. Touch **[Save]**.
9. Touch **[Dynamic Addressing]**.
10. Touch **[Disabled]** to disable DHCP.
11. Touch **[Save]**.
12. Touch **[IP Address/Host Name]**.
13. Touch button under the **[IPv4 Address]** heading, enter the IP Address using the on-screen keypad.
14. Touch **[Host Name]**. Type the host name EXACTLY as you want it to appear. To access more characters, touch **[123]** on the user interface.
15. Touch **[Save]**, then touch **[Close]**.
16. Touch **[Subnet and Gateway]**.
17. Touch **[Subnet Mask]**, enter the Subnet Mask address using the on-screen keypad.
18. Repeat this process for the **IP Gateway**. When you are finished, touch **[Save]** to accept the changes and return to the TCP/IP Settings screen.
19. Touch **[Close]** twice to return to the feature menu.
20. Touch **[Advanced Settings]**.
21. Touch **[Continue]**.
22. Touch **[HTTP Settings]** and ensure **Enable** is selected. If not, touch **[Enable]**.
23. Touch **[Save]**, then touch **[Close]**, to return to the **Tools** menu.

DNS/DDNS Configuration

24. Touch **[TCP/IP Settings]**.
25. Touch **[DNS Configuration]**. This feature will be inaccessible (grayed out) if TCP/IP protocol is not enabled.
26. Touch the **[Domain Name]** keyboard button.
27. Touch the button under **Domain Name**.
28. Touch the **[Clear Text]** button to remove the default name before entering the new name using the on screen keyboard.
29. Touch **[Save]**.
30. Touch **[Close]**.
31. Touch **[Preferred DNS Server]**.
32. Touch the button under **Preferred DNS Server #1**, enter the *DNS Server IP Address* using the on-screen keypad.
33. Touch **[Save]**, then touch **[Close]**.
34. Touch **[Alternate DNS Servers]** if required.
35. Touch the button under **Alternate DNS Server**, enter the *Alternate DNS Server IP Address* using the on-screen keypad.
36. Touch **[Save]**.

    Note

    If DHCP is enabled, the Alternate DNS server information is not available as a feature summary.

37. Touch **[Close]**.

Enable Dynamic DNS Registration

Note
If your DNS server does not support dynamic updates, then this function does not need to be enabled.

38. Touch **[Dynamic DNS Registration]**.
39. Click on **[Enable]**, then **[Save]**.
40. Touch **[Close]** three times.
41. Press the **[Log In/Out]** button, touch **[Logout]** to exit **Tools** mode.

Configure Dynamic Addressing

Information Checklist

Before starting the installation procedure, please ensure that the following items are available and/or the tasks have been performed:

- Existing operational network utilizing the TCP/IP protocol.
- DHCP or BOOTP Server should be available on the network.
- Device must be connected to the network via Ethernet Cable.

Installation via DHCP (Dynamic Host Configuration Protocol)

DHCP is enabled on the device by default. If the device is connected to the network, the TCP/IP information will be configured when the device is powered on and no further configuration is required.

Print a Configuration Report to verify that TCP/IP information is correct.

1. Press the **<Machine Status>** button on the device.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

The Confirmation Report is printed, verify the TCP/IP information.

Installation via BOOTP or DHCP

Ensure your device is connected to the network with Ethernet cabling.

1. Go to the device and press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, and then the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[TCP/IP Settings]**.
6. Touch **[Dynamic Addressing]**. By default, DHCP is selected.
7. Select the required Dynamic Addressing method:
   - **[BOOTP]**
   - **[DHCP]**
8. Touch **[Save]**.
9. Touch **[Close]**.

10. Press the **[Log In/Out]** button, touch **[Logout]** to exit **Tools** mode.

IPv4

Configure TCP/IP Settings using Internet Services

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

   Note

   TCP/IP and HTTP should have been initially configured, refer to Enable TCP/IP and HTTP at the Device on page 2-5 of this guide.

2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Ensure that **[IPv4]** is selected.
9. The **Protocol** will be **[Enabled]** to enable the TCP/IP protocol.

   Note

   If you do not check the **Protocol** Enabled checkbox you will not be able to access Internet Services. TCP/IP must then be enabled from the device's user interface.

CAUTION

Disabling TCP/IP or changing the IP Address will affect NetBIOS/IP, LPR/LPD, FTP, SNMP, and Raw TCP/IP printing. If TCP/IP is disabled, Internet Services will not be available until TCP/IP is enabled from the control panel of the device. If you change the IP address, you must reference the new address within your web browser to locate the device.

10. Enter a unique **[Host Name]** for your device.
11. Select the desired method for obtaining a Dynamic IP address from the **[IP Address Resolution]** drop-down list, or select **[Static]** to give the device a static IP address.
12. If you select **[Static]**, type the IP addresses that apply in **[Machine IP Address, Subnet Mask]**, and **[Gateway Address]**.

    Note

    If **BOOTP** or **DHCP** address resolution mode is selected, you cannot change the IP address, Subnet Mask, or default gateway. If RARP address resolution mode is selected, you cannot change the IP address. Select **[Static]** if you wish to disable dynamic addressing.

Domain Name

13. Enter a valid **[Domain Name]**.

DNS Configuration

14. Enter an IP address for the **[Preferred DNS Server]**. Enter an IP address for **[Alternate DNS Servers 1]** and **[Alternate DNS Servers 2]**.
15. Check the **[Enable]** box to enable **[Dynamic DNS Registration (DDNS)]**.

Note

If your DNS Server does not support dynamic updates there is no need to enable DDNS.

16. Check the **[Enable]** box for **Release Registration** in the **DHCP/DDNS** area ONLY if you wish to release this device's IP address upon reboot. Default is unchecked.
17. Check the **[Enable]** box for **Self Assigned Address**, in the Zero-Configuration Networking area, to support communicating with other devices using 169.254/16 IPv4 addressing, over the same physical or logical link (such as in ad hoc, or isolated (non- DHCP) networks). Refer to the IETF website for zeroconf details.
18. Check the **[Enable]** box for **Multicast DNS** to resolve host names to IPv4 addresses without using a conventional DNS server.

DHCP/DDNS

19. Check the **[Enable]** box for **[Release Registration]** if you want the device to release DHCP resources when the device is powered down.

Zero-Configuration Networking

20. Check the **[Enable]** box for **[Self Assigned Address]** to allow the device to assign itself an IP address of 169.254.*x.x*. This is useful in situations where the device cannot connect to the DHCP server to obtain an IP address.
21. Check the **[Enable]** box for **[Multicast DNS]** if you want to enable the device to perform DNS queries over IP Multicast. This is essential for the Apple Rendezvous protocol to map a host name to an IP address, used to advertise the services of the device.
22. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
23. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

Note

Changing the device IP Address will impact other protocols: NetBIOS/IP, LPR/LPD, FTP, SNMP and Raw TCP/IP Printing. These protocols will need to reference the new IP Address.
Disabling TCP/IP will impact other protocols: NetBIOS/IP, LPR/LPD, FTP, SNMP and Raw TCP/IP Printing. This web user interface will be disabled until TCP/IP is re-enabled from the local user interface.

IPv6

Note

IPv6 is optional. It may be used in addition to, or in place of IPv4.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

Note

TCP/IP and HTTP should have been initially configured refer to Enable TCP/IP and HTTP at the Device on page 2-5 of this guide.

2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Ensure that **[IPv6]** is selected.

9. Check the **[Enable]** box for **Protocol** to enable the TCP/IP protocol.

   Note

   If you do not check the **Protocol** Enabled box you will not be able to access Internet Services. TCP/IP must then be enabled from the device's user interface.

10. The Host Name is populated when configured at the IPv4 screen. If you change the Host Name here it will also change it for IPv4.
11. Enter the required **[Domain Name]**.
12. **Stateless Addresses**: The Link-Local Address is automatically populated.
    a. Check the **[Enable]** box for **[Use Router Supplied Prefixes]** if router advertisements are used.
13. **Default DHCP (Dynamic Host Configuration Protocol) Settings**
    The device performs auto-address DHCP configuration every time it powers up. This is used for neighbour discovery and address resolution on the local IPv6 subnet.
    However, you can choose to use manual configuration, automatic configuration or a combination of automatic and manual configuration.
    a. Select one of the following options:
    - **[Use DHCP as directed by a router]** - this option is fully automatic. The DHCPv6 Address will be obtained and displayed on the screen.
    - **[Always Enable DHCP]** - this option is fully automatic. The DHCPv6 Address will be obtained and displayed on the screen.
    - **[Never use DHCP]** - when this option is selected, you must configure the Manual Address Options and DNS separately.

DNS Configuration

14. Enter an IP address for the **[Preferred DNS Server]**. Enter an IP address for **[Alternate DNS Server1]** and **[Alternate DNS Server2]**.
15. Check to enable **[Prefer IPv6 Address over IPv4]**.

    Note

    If your DNS Server does not support dynamic updates there is no need to enable DDNS.

Manual Address Options

The device can be configured with up to 4 manual IPv6 addresses.

16. Check the **[Enable]** box for **Manual Address** if required.
17. The **Router Prefix** is derived from router advertisements. Select a router address prefix from the list supplied in the **[Router Prefix]** menu to populate the prefix for manual entry address.
18. Click on the **[Add]** button to add your address.
19. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
20. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

Supporting LPR Printing

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

   Note

   TCP/IP and HTTP should have been initially configured, refer to Enable TCP/IP and HTTP at the Device on page 2-5 of this guide and follow the steps provided.

2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[LPR/LPD]** in the directory tree.
8. Check the **[Enable]** box to enable LPR/LPD.

   Note

   Disabling LPR/LPD will affect clients printing to the device over TCP/IP using the LPR printing port.

9. In the **Port Number**, enter an LPR/LPD port number. The default is 515.
10. In the **Advanced Settings** area, check the **[Enabled]** box to enable **PDL Switching**. PDL switching allows the device to process print jobs which contain two or more printer languages, for example: PCL and PostScript, or ASCII and PostScript.
11. Check the **[Enabled]** box to enable **PDL banner page attributes override LPR control file attributes for job name and owner**. This feature allows you to replace the standard information displayed on a banner page, and substitute the user name and job name taken from the print job.
12. Select the required option from the **[Place temporary hold on which jobs:]** drop-down menu. This feature allows you to set the device to hold certain jobs before printing, until the complete job is received. This delay helps to ensure that the banner page information prints correctly. Some banner sheet information is contained in the job's control file which may not always be the first part of a print job the device receives. The following options are available:
    - **Only those with data file received 1st** - The device holds the job if the job's data file is received first. This ensures the device waits to receive the job's control file information so that the banner sheet contains accurate information.
    - **All (consistent with older implementations)** - This option puts all jobs on hold. All data is received before a job begins to print. This setting can cause jobs to print slowly but will result in accurate banner sheet information.
    - **None (Use printer's default banner sheet job name if data file 1st)** - The device will not wait to receive the job control information. This selection may cause banner sheet information to print incorrectly.
13. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
14. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

Configure Raw TCP/IP Printing

Note

TCP/IP must be enabled before Raw TCP/IP Printing is enabled.

Raw TCP/IP is a printing method used to open a TCP socket-level connection, over Port 9100, to stream a print-ready file to the printer's input buffer, and then to close the connection after sensing an End Of Job indicator in the Page Description Language, or after expiration of a preset timeout value. Port 9100 printing does not require a Line Printer Request (LPR) from the workstation, or the use of a Line Printer Daemon (LPD) running on the printer. Raw TCP/IP printing is selected in Windows 2000 as the Standard TCP/IP port.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address or Location field. Press **[Enter]**.
2. Click on the **[Properties]** tab.

3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. Ensure the **[Enabled]** box is checked to enable Raw TCP/IP Printing Protocol.
9. Leave the **[TCP Port Number]** set to 9100 for Port 1. If two additional ports are available, click **[Default All]** to see if they set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
10. Leave the **[Bidirectional]** checkboxes and **[Maximum Connections]** settings at their default values.
11. Set the **[End of Job Timeout]** to the number of seconds to wait before processing a job without an End Of Job indicator.
12. Leave the **[PDL Switching]** Enabled checkbox at its default value.
13. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values, or **[Default All]** to enter printer defaults for all settings (recommended).
14. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you restart the device.

15. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
16. Click the **[Reboot Machine]** button and click **[OK]** to reboot the device. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time

Configure SLP

Configure SLP (if needed to support CUPS, Mac OS, and NetWare).

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[SLP]** in the directory tree.
8. Check the **[Enabled]** box to enable Service Location Protocol (SLP).
9. Enter an **[IP address]** for the Directory Agent, if required.
10. Enter the required name(s) for **[Scope 1,2,3]**.
11. Select the Message type from the drop down menu for **[Multicast or Broadcast]**.
12. Enter a value for **[Multicast Radius]** (0-255).
13. Enter a value for **MTU** to set the Maximum Transmission Unit (484 - 32768), with 1400 as the default. This allows you to set the maximum packet size for SLP.
14. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.

    Note

    The settings are not applied until you restart the device.

15. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

SNMP

Allows you to configure the following options when accessing the device via SNMP.

SNMP (Simple Network Management Protocol) settings can be configured via Internet Services. You can also enable or disable Authentication Failure Generic Traps on the device. SNMPv3 can be enabled to create an encrypted channel for secure device management.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[SNMP]** in the directory tree.

Configure SNMP v1/v2c

Note

For security purposes, Xerox recommends that the administrator changes the SNMP v1/V2c public/ private community strings from their default string names to random string names.

8. Check to ensure the **[Enable SNMP v1/v2c Protocols]** box is selected.
9. Click on the **[Edit SNMP v1/v2c Properties]** button.
10. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
11. Click on the **[Login]** button.
12. Enter a name for the **[GET Community Name]**. The default is public.
13. Enter a name for the **[SET Community Name]**. The default is private.

Note

Changes made to the GET or SET community names for this device will require corresponding GET or SET community name changes for each application which uses the SNMP protocol to communicate with this device (for example, Xerox PrinterMap, Xerox CentreWare, any 3rd party network management applications).

14. Enter a name for the default **[TRAP Community Name]**. The default is **SNMP_trap**.

Note

The Default TRAP community name is used to specify the default community name for all traps generated by this device. The Default TRAP community name can be overridden by the TRAP community name specified for each individual TRAP destination address. The TRAP community name for one address may not be the same TRAP community name specified for another address.

15. Click on the **[Apply]** button to accept the changes.

Configure SNMP v3

Note

SSL (Secure Socket Layer) must be enabled before you can configure SNMP v3. Click the **[Configure HTTPS]** link on the SNMP Internet Services screen to complete this task. Once SSL is enabled, return to the SNMP screen.

Before, enabling the HTTP Security Mode, the device **must** have a Machine Digital Certificate configured. For information on Machine Digital Certificate, see Machine Digital Certificate Management on page 8-9.

16. From the **[Protocols]** link, select **[HTTP]** in the directory tree.
17. Select enable for the **[Secure HTTP (SSL)]** option.
18. Change the HTTP **[Port Number]** if required. The default is 80.
19. Click on the **[Apply]** button to accept the changes.
20. Check the **[Enable SNMP v3 Protocol]** box to enable **SNMP v3**.
21. Click on the **[Edit SNMP v3 Properties]** button.
22. Select the **[Create]** button within the **Administrator Account** area to create an administrator account.
23. Enter the required data in the **[Authentication Key]** text box.
24. Enter the required data in the **[Privacy Key]** text box.
25. Select the **[Create]** button within the **[Print Drivers Account]** area.
26. When you have finished configuring the settings, click the **[Apply]** button.

SSDP

Allows you to configure the SSDP (Simple Service Discovery Protocol) for Universal Plug and Play settings on the device.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[SSDP]** in the directory tree.
8. Check the **Protocol [Enabled]** box to enable SSDP.
9. Enter a setting in the **[Cache Control]** box.
10. Enter a setting in the **[Time to Live]** box.
11. Click on the **[Apply]** button to accept the changes.

Microsoft Networking and WINS (Windows Internet Naming Service)

Configure Microsoft Networking

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.

4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Microsoft Networking]** in the directory tree.
8. Check the **[Enabled]** box under **Protocol** to enable Microsoft Networking.
9. Enter the maximum number of connections allowed in **[Maximum Connections]**. The range is 10 - 30.
10. Enter the Connection Timeout in the available box. The range is 1 - 32767 seconds.
11. Enter the workgroup name in the **[Workgroup]** box.
12. Enter the **[SMB Host Name]** and type a descriptive comment in **[SMB Host Name Comment]** (optional).
13. Type the **[Share Name]** and type a descriptive comment in **[Share Name Comment]**.

Configure WINS (if used)

When running WINS the device registers its IP address and NetBIOS Hostname with a WINS server. WINS allow the device to communicate using hostname only, removing a significant overhead from the systems administrators.

WINS server address is stored in the file **/smart/etc/wins.**Name.

It is possible to manually enable WINS and configure primary and secondary WINS servers through Internet Services.

14. Check the **[Enabled]** box under **Protocol** to enable WINS.
15. Enter the IP Address in the **[Primary Server IP Address]** of a Primary Server.
16. Enter the IP Address in the **[Secondary Server IP Address]** of a Secondary Server.

    Note

    If DHCP is configured, WINS IP Address(es) will be overridden.

17. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.

    Note

    The settings are not applied until you reboot the device.

18. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

AppleTalk

Enabling AppleTalk on the device

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar. Press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[AppleTalk]** in the directory tree.

8. Check the **[Enabled]** box to enable the Protocol.
9. Type a name for the device in **[Printer Name]**. The default name is XRX_MAC address.

   Note

   The default local zone is identified as "*". This should only be changed if you have defined zones on your network.

10. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
11. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you reboot the device.

Create an IPP Printer (Internet Printing Protocol)

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 2-5, so that the web user interface (Internet Services) can be accessed.
- Ensure that the DNS settings are configured.

Enable Port 9100 as additional support for HTTP (IPP) printing

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. Ensure the **[Enabled]** box is checked to enable Raw TCP/IP Printing Protocol.
9. Leave the **[TCP Port Number]** set to 9100 for Port 1. If two additional ports are available, click **[Default All]** to see if they are set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
10. Leave the **[Bidirectional]** checkboxes and **[Maximum Connections]** settings at their default values.
11. Set the **[End of Job Timeout]** to the number of seconds to wait before processing a job without an End Of Job indicator.
12. Leave the **[PDL Switching]** checkbox enabled at its default value.
13. Click on the **[Apply]** button to accept the changes.
14. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you restart the device.

Create an IPP Printer at your Workstation

Verify the correct software is loaded

1. At the Desktop, right-click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click the **[Local Area Connection]** icon.
4. Click **[Properties]**.
5. Verify that the **[Internet Protocol (TCP/IP)]** protocol has been loaded.

Install the Printer Driver

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]** (Windows 2000) or **[Printers and Faxes]** (Windows XP). The Vista path is *Start\Control Panel\Printer(s)*.
2. Double-click the **[Add Printer]** icon and click **[Next]**.
3. Verify that **[Network Printer]** is selected and click **[Next]**.
4. The **[Locate Your Printer]** (Windows 2000) or **[Specify a Printer]** (Windows XP) screen will appear.
5. To create an IPP printer select **[Connect to a printer on the Internet or on your intranet]**.
6. Type ***HTTP://...*** followed by the printer's fully qualified Domain name or IP address in the URL field. The Printer Name can be either the Host Name or the SMB Host Name as shown on the device configuration report, depending on the name resolution used by your network (WINS or DNS).
7. Click **[Next]**.
8. Select **[Have Disk]** and browse to the location of the printer driver (.INF).
9. Click **[OK]** to install the printer driver.
10. Select the Printer Model and Click [Next].
11. Select **[Yes]** if you wish to make this the default printer.
12. Select **[Yes]** to print a Test Page. Verify that it prints at the device.
13. Click **[Finish]**.

Internet Services

Once installed an IPP printer should provide a link directly to the Internet Services web pages.

To Access Internet Services

1. From the **[Start]** menu select **[Settings]** and then **[Printers]**.
2. Click on the device printer icon and a '**Get More Info'** link will appear in the left hand pane of the window.
3. Click the **[Get More Info]** link to go to straight to the device home page.

You have completed the installation of an IPP port and printer drivers.

At the Windows 2000 Desktop

1. Right-click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click on the network connection you want to configure AppleTalk on, and then click **[Properties]**. The Connection Properties dialog box opens.
4. On the General tab, if the AppleTalk Protocol is in the list of installed protocols, make sure that it is selected. If the AppleTalk protocol is not listed, install it using the documentation provided by Microsoft. Then return to the next step in this document.

5. Click **[Start]**, **[Settings]**, then **[Printers]**.
6. Double-click the **[Add Printer]** icon to start the Add Printer Wizard.
7. Click **[Next]**.
8. Click **[Local Printer]**. Deselect the **Automatically detect and install my Plug and Play printer** option.
9. Click **[Next]**.
10. Click **[Create a New Port]**.
11. Select **[AppleTalk Printing Devices]** and click **[Next]**.
12. In the Available AppleTalk Printing Devices box, click the printer you want to connect to. It may be necessary to double-click the required Zone to locate the printer. Click **[OK]**.

    Note

    You may be asked whether you want to capture the AppleTalk print device. If you are prompted to do this and you are unsure how to respond, click the Help button and read the help file for an explanation of capturing AppleTalk print devices.

    Capturing the printer may prevent other computers from printing to this printer. For more information refer to Microsoft.

13. Click **[Have Disk]**. Load the CentreWare Print and Fax Drivers CD into your CD drive.
14. Click **[Browse]** and locate the CD drive.
15. Locate the folder containing printer drivers on the CD and select the required Windows 2000 printer driver.
16. Select **[Open]**.
17. Select **[Open]** again, if necessary.
18. Select **[OK]**.
19. Select your printer model from the list and click **[Next]**.
20. Type a name for the printer (or accept the default name), and then click **[Next]**.
21. If you want this to be your default printer click **[Yes]**.
22. Click **[Next]**.
23. If you want to share this printer from your computer, click **[Share As:]**. Enter a share name (or accept the default name), then click **[Next]**.
24. If you want to print a test page, click **[Yes]**, then click **[Finish]**.

Windows XP

Configure TCP/IP and SLP Settings

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

   Note

   TCP/IP and HTTP should have been initially configured, refer to Enable TCP/IP and HTTP at the Device on page 2-5 of this guide and follow the steps provided.

2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Check the **[Enabled]** box to enable the TCP/IP protocol.

CAUTION

Disabling TCP/IP or changing the IP Address will affect NetBIOS/IP, LPR/LPD, FTP, SNMP, and Raw TCP/IP printing. If TCP/IP is disabled, Internet Services will not be available until TCP/IP is enabled from the control panel of the device. If you change the IP address, you must reference the new address within your web browser to locate the device.

9. Enter a unique **[Host Name]** for your device.
10. Select the desired method for obtaining a Dynamic IP address from the **[IP Address Resolution]** drop-down list, or select Static to give the device a static IP address.
11. If you select **[Static]**, type the IP addresses that apply in **[Machine IP Address, Subnet Mask]**, and **[Gateway Address]**.

    Note

    If **BOOTP** or **DHCP** address resolution mode is selected, you cannot change the IP address, Subnet Mask, or default gateway. If **RARP** address resolution mode is selected, you cannot change the IP address. Select **[Static]** if you wish to disable dynamic addressing.

Domain Name

12. Enter a valid **[Domain Name]**.

DNS Configuration

13. Enter an IP address for the **[Preferred DNS Server]**. Enter an IP address for **[Alternate DNS Servers 1]** and **[2]**.
14. Check the box to enable **[Dynamic DNS Registration (DDNS)]**. If your DNS Server does not support dynamic updates there is no need to enable DDNS.
15. Check the **[Enable]** box under DHCP/DDNS Release Registration ONLY if you wish to release this device's IP address upon reboot. Default is unchecked.

16. Check the **[Enabled]** box for Self Assigned Address, under Zero-Configuration Networking, to support communicating with other devices using 169.254/16 IPv4 addressing, over the same physical or logical link (such as in ad hoc, or isolated (non-DHCP) networks). Refer to the IETF website for zeroconf details.
17. Check the **[Enabled]** box for Multicast DNS to resolve host names to IPv4 addresses without using a conventional DNS server.

Supporting LPR Printing

18. Select **[LPR/LPD]** in the directory tree.
19. Check the **[Enabled]** box to enable LPR/LPD.

Configure SLP (if needed to support CUPS, Mac OS, and NetWare)

20. Select **[SLP]** in the directory tree.
21. Check the **[Enabled]** box to enable Service Location Protocol (SLP).
22. Enter an **[IP address]** for the Directory Agent, if required.
23. Enter the required name(s) for **[Scope 1,2,3]**.
24. Select the Message type from the drop down list for **[Multicast or Broadcast]**.
25. Enter a value for **[Multicast Radius]** (0-255).
26. Enter a value for MTU to set the Maximum Transmission Unit (484 - 32768), with 1400 as the default. This allows you to set the maximum packet size for SLP.
27. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
28. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you restart the device.

29. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
30. Click the **[Reboot Machine]** button and click **[OK]** to reboot the device. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time

Configure Raw TCP/IP Printing

Note

TCP/IP must be enabled before Raw TCP/IP Printing is enabled.

Raw TCP/IP is a printing method used to open a TCP socket-level connection, over Port 9100, to stream a print-ready file to the printer's input buffer, and then to close the connection after sensing an End Of Job indicator in the Page Description Language, or after expiration of a preset timeout value. Port 9100 printing does not require a Line Printer Request (LPR) from the workstation, or the use of a Line Printer Daemon (LPD) running on the printer. Raw TCP/IP printing is selected in Windows 2000 as the Standard TCP/IP port.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.

8. Ensure the **[Enabled]** box is checked to enable Raw TCP/IP Printing.
9. Leave the **[TCP Port Number]** set to 9100 for Port 1. If two additional ports are available, click **[Default All]** to see if they set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
10. Leave the **[Bidirectional]** and **[Maximum Connections]** settings at their default values.
11. Set the **[End of Job Timeout]** to the number of seconds to wait before processing a job without an End Of Job indicator.
12. Leave the **[PDL Switching] Enabled** box at its default value.
13. Click on the **[Apply]** button to accept the changes, **[Undo]** to return the settings to their previous values, or **[Default All]** to enter printer defaults for all settings (recommended).
14. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you restart the device.

15. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
16. Click the **[Reboot Machine]** button and click **[OK]** to reboot the device. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time

Create an IPP Printer (Internet Printing Protocol)

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

1. Ensure TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 2-5, so that the web user interface (Internet Services) can be accessed.
2. Ensure that the DNS settings are configured.

Enable Port 9100 as additional support for HTTP (IPP) printing

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. Ensure the **[Enabled]** box is checked to enable Raw TCP/IP Printing.
9. Leave the **[TCP Port Number]** set to 9100 for Port 1. If two additional ports are available, click **[Default All]** to see if they set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
10. Leave the **[Bidirectional]** and **[Maximum Connections]** settings at their default values.
11. Set the **[End of Job Timeout]** to the number of seconds to wait before processing a job without an End Of Job indicator.
12. Leave the **[PDL Switching]** Enabled box at its default value.
13. Click on the **[Apply]** button to accept the changes.

14. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you restart the device.

15. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
16. Click the **[Reboot Machine]** button and click **[OK]** to reboot the device. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time
17. A Configuration Report should have printed (by default) when the device rebooted.
18. If the Configuration Report did not print, go to the device:
    - Press the **<Machine Status>** button.
    - Touch the **[Machine Information]** tab.
    - Touch **[Information Pages]**.
    - Touch **[Configuration Report]**.
    - Touch **[Print]**, then touch **[Close]**.
19. Review the settings for Raw TCP/IP Printing under the heading TCP/IP Settings. These settings should read as follows:
    a. Raw TCP/IP Printing Enabled: Enabled
    b. Raw TCP/IP Port Number: 9100

Create an IPP Printer at your Workstation

Verify the correct software is loaded

1. At your Workstation, right-click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click on the **[Local Area Connection]** icon.
4. Click **[Properties]**.
5. Verify that the **[Internet Protocol (TCP/IP)]** protocol has been loaded.

Install the Printer Driver

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]** (Windows 2000) or **[Printers and Faxes]** (Windows XP). The Vista path is Start\Control Panel\Printer(s).
2. Double-click the **[Add Printer]** icon and click **[Next]**.
3. Verify that **[Network Printer]** is selected and click **[Next]**.
4. The **[Locate Your Printer]** (Windows 2000) or **[Specify a Printer]** (Windows XP) screen will appear.
5. To create an IPP printer select **[Connect to a printer on the Internet or on your intranet]**.
6. Type **HTTP:// followed by the printer's fully qualified Domain name or IP address** in the URL field. The Printer Name can be either the Host Name or the SMB Host Name as shown on the device Configuration Report, depending on the name resolution used by your network (WINS or DNS).
7. Click **[Next]**.
8. Select **[Have Disk]** and browse to the location of the printer driver (.INF).
9. Click **[OK]** to install the printer driver.
10. Select the Printer Model and Click **[Next]**.
11. Select **[Yes]** if you wish to make this the default printer.
12. Select **[Yes]** to print a Test Page. Verify that it prints at the device.
13. Click **[Finish]**.

Internet Services

Once installed, an IPP printer will provide a link directly to the Internet Services web pages.

To Access Internet Services

1. From the **[Start]** menu select **[Printers and Faxes]**.
2. Click on the device printer icon and a Get More Info link will appear in the left hand pane of the window.
3. Click the **[Get More Info]** link to go to straight to the device home page.

You have completed the installation of an IPP port and printer drivers.

Configure Microsoft Networking and WINS (Windows Internet Naming Service)

Configure Microsoft Networking

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Microsoft Networking]** in the directory tree.
8. Check the **[Enabled]** box to enable Microsoft Networking.
9. Select **[TCP/IP]** or **[NetBIOS]** from the **[Transport]** drop-down list.
10. Enter the maximum number of connections allowed in **[Maximum Connections]**. The range is 10 - 30.
11. Enter the Connection Timeout in the available box. The range is 1 - 32767 seconds.
12. Enter the workgroup name in the **[Workgroup]** box.
13. Enter the **[SMB Host Name]** and type a descriptive comment in **[SMB Host Name Comment]** (optional).
14. Type the **[Share Name]** and type a descriptive comment in **[Share Name Comment]** (optional).

Configure WINS (if used)

1. Check the **[Enabled]** box to enable WINS.
2. Enter the IP Address of a Primary WINS server, and port.
3. Enter the IP Address of a Secondary WINS server and port.

   Note

   If DHCP is configured, WINS IP Address(es) will be overridden.

4. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
5. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.

   Note

   The settings are not applied until you restart the device.

6. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
7. Click the **[Reboot Machine]** button and click **[OK]** to reboot the device. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time

Apple Talk

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- An existing operational AppleTalk network with Macintosh workstation computers equipped with Ethernet network interface cards.
- The AppleTalk Name you wish to assign to your printer.
- The AppleTalk Zone (if used) in which your printer will reside.
- Ethernet Cable.
- The CentreWare Print and Fax Drivers CD (delivered with your device). Review any README file contained with the printer drivers.

Enabling AppleTalk on the device

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[AppleTalk]** in the directory tree.
8. Check the **[Enabled]** box to enable the AppleTalk Protocol.
9. Type a name for the device in **[Printer Name]**. The default name is XRX_MAC address.

   Note

   The default local zone is identified as "*". This should only be changed if you have defined zones on your network.

10. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
11. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you restart the device.

Install the Print Driver

Refer to the Print and Fax Drivers Guide for Macintosh on the CentreWare Print and Fax Drivers CD for detailed instructions.

1. View the Configuration Report and note the *Name* given to the device under AppleTalk Settings.

At the Macintosh Workstation

2. Load the CentreWare Print and Fax Drivers CD-ROM into your CD drive.
3. Open the CD and locate the **[Drivers]** folder.

4. Locate and open the **[Mac]** folder.

Instructions for Version 10.x (OS X)

1. Double-click to open the folder containing the drivers for version 10.x.
2. Double-click to open the **[machine model.dmg]**.
3. Double-click to open the **[machine model.pkg]** file.
4. When the Welcome screen displays, click **[Continue]**.
5. Click **[Continue]**, then **[Agree]** to accept the License Agreement.
6. Select the required disk (if necessary) where you want to install the printer. Click **[Continue]**.
7. Click **[Install]**.
8. Click **[Close]**, and restart the workstation.
9. When the workstation has restarted, double click the hard drive icon.
10. Double-click the **[Applications]** icon.
11. Double-click the **[Utilities]** folder.
12. Double-click **[Print Center]** icon.
13. Double-click **[Add]** to add a new printer.
14. Select AppleTalk as your network protocol.
15. Select the required AppleTalk zone.
16. Select the printer that you wish to set up.
17. Select the Printer Model (that is, choose the PPD for your printer).
18. Click **[Add]**.
19. Print a document from an application to verify that the printer is installed correctly.

View the Macintosh Printer Utility on the CentreWare Print and Fax Drivers CD.

CentreWare is a suite of applications used for installing, maintaining and using the Xerox devices. CentreWare Macintosh Printer Utility is a CentreWare application that enables network administrators to rename and rezone Xerox systems that are configured for AppleTalk connectivity. Locate the CentreWare Print and Fax Drivers CD-ROM delivered in the CentreWare Network Services Pack with your device follow the instructions contained in the CentreWare Print and Fax Drivers Guide for Macintosh.

Apple Macintosh (TCP/IP)

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- An existing operational TCP/IP network with Macintosh workstation computers equipped with Ethernet network interface cards.
- Macintosh Operating System of 10.x or higher.
- A live network drop and Ethernet Cable for the Macintosh workstation.
- The printing device should already be configured with a static IP address (preferred), Subnet Mask, and Gateway Address, as well as with a Host Name.
- The CentreWare Print and Fax Drivers CD (delivered with your device). Review any README file contained with the printer drivers.

Enabling TCP/IP on the device

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[TCP/IP]** in the directory tree.
8. Verify that the printing device has been configured with a static IP address (preferred), Subnet Mask, Gateway Address, and Host Name.
9. Verify that the Domain Name for your network has been supplied, and that DNS is enabled and configured to resolve Host Names to IP Addresses.

   Note

   Changing the device IP Address will impact other protocols: NetBIOS/IP, LPR/LPD, FTP, SNMP and Raw TCP/IP Printing. These protocols will need to reference the new IP Address.
   Disabling TCP/IP will impact other protocols: NetBIOS/IP, LPR/LPD, FTP, SNMP and Raw TCP/IP Printing. This web user interface will be disabled until TCP/IP is reenabled from the local user interface.

10. If any of the above items are incorrectly set, reset them and click on the **[Apply]** button.
11. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
12. Select **[LPR/LPD]** in the directory tree and verify that the **Protocol** is Enabled, and the **Port Number** is set to 515.

    Note

    The settings are not applied until you restart the device.

13. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
14. Click the **[Reboot Machine]** button and click **[OK]** to reboot the device. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.
15. A Configuration Report should have printed by default when the device rebooted. Look at the report to verify TCP/IP settings.
16. If the Configuration Report did not print, go to the device:
    - Press the **<Machine Status>** button.
    - Touch the **[Machine Information]** tab.
    - Touch **[Information Pages]**.
    - Touch **[Configuration Report]**.
    - Touch **[Print]**, then touch **[Close]**.

Select the PPD - PostScript® Printer Definition

1. Insert the CentreWare Print and Fax Drivers CD into your CD drive.
2. Double-click the printer icon on your desktop.
3. Select **[Printing]**.
4. Select **[Change Setup]**.
5. Select **[Change]**.
6. Locate the **[Drivers]** folder on the CD.
7. Select the appropriate PPD for OS 10.x.

8. Select the options according to those installed on your device.
9. Click **[OK]**.
10. Print a document from an application to verify that the printer is installed correctly.

Set up LPR (Line Printer Remote) Printing in Mac OSX

1. Load the CentreWare Print and Fax Drivers CD-ROM into your CD drive.
2. Open the CD and select the required language.
3. Double-click to open the **[Drivers]** folder.
4. Double-click to open the **[Mac]** folder.

   Note

   There may be more than one Print and Fax Drivers CD. If the Mac folder does not appear, check for another Print and Fax Drivers CD.

5. Double-click to open the folder containing the drivers for version 10.x.
6. Double-click to open the **[machine model.dmg]** file.
7. Double-click to open the **[machine model.pkg]** file.
8. The Welcome to the Installer dialog box appears. Click **[Continue]**
9. Click **[Continue]** and then **[Agree]** to accept the License Agreement.
10. Select the required disk (if necessary) where you want to install the printer. Click **[Continue]**.
11. Click **[Install]**.
12. Click **[Close]**.
13. Restart your computer.
14. When your computer has restarted, open Print Centre. To do this:
15. Double-click the hard drive icon on the desktop.
16. Double-click to open **[Applications]**
17. Double-click to open **[Utilities]**.
18. Double-click to open **[Print Center]**.
19. Double-click **[Add]** to add a new printer.
20. Select **[IP Printing]** from the menu.
21. Enter the IP address of the printer.
22. Select **[Xerox]** from the printer model list.
23. Select Xerox ColorQube 9201/9202/9203 (according to your model) from the model name list.
24. Click **[Add]**.
25. Print a document from an application to verify that the printer is installed correctly.

View the Macintosh Printer Utility on the CentreWare Print and Fax Drivers CD

CentreWare is a suite of applications used for installing, maintaining and using the Xerox devices. CentreWare Macintosh Printer Utility is a CentreWare application that enables network administrators to rename and rezone Xerox systems that are configured for AppleTalk connectivity. Locate the CentreWare Print and Fax Drivers CD-ROM delivered in the CentreWare Network Services Pack with your device and follow the instructions contained in the CentreWare Print and Fax Drivers Guide for Macintosh.

NetWare

Information Checklist

Before starting the installation procedures, please ensure the following items are available or have been performed:

- An existing operational NetWare network.
- Login to a NetWare file server/tree as Supervisor/Administrator or have the equivalent privileges.
- Ensure the device is connected to the network via Ethernet cable.
- Set up a print server object using NWADMIN. Refer to the documentation supplied by Novell to complete this task. Record precisely (observe upper and lower case, dot notation) the NDS Tree, NDS Context Name, frame type, Print Server Name and the Print Server password assigned. If your printer services queues on multiple file servers, the Print Server name and password must be the same on all file servers.

Configure NetWare Settings

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Connectivity]** link.
5. Click on the **[Protocols]** link.
6. Select **[NetWare]** in the directory tree.
7. Check the **[Enabled]** box to enable NetWare protocol.
8. Select the required **Filing Transport** drop down menu.
9. Select the required **[Frame Type]** from the drop down list.
10. Type a polling rate for the print server in **[Queue Poll Interval]** (1 - 240 seconds. The default is 5).
11. Enter the **[Print Server Name]** The default name is XRX_MAC address.
12. Enter the print server password in the **[New Print Server Password]** box, then re-enter it in the **[Retype New Print Server Password]** box. Place a check in the **[Select to save new password]** box.

Service Advertising Protocol (SAP)

13. Check the **[Enabled]** box if you wish to enable SAP protocol.
14. Enter the **[SAP Frequency]** (from 15 - 300 seconds or enter 0 for none. The default is 60).

Bindery Settings

15. If using NetWare in Bindery mode, enter the names of up to four primary **[File Servers]** for the device in the Bindery Settings box.

NetWare Directory Services (NDS)

1. If using NetWare NDS (NetWare Directory Services), enter a directory tree and context for the device in **[NDS Tree]** and **[NDS Context]** in the Netware Directory Services (NDS) box.

Note

That you can also select the IP Address or Host Name radio buttons to specify the server used in the IP environment.

2. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
3. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.

Note

The settings are not applied until you restart the device.

NDPS/NEPS

For The Xerox NDPS/NEPS Agent, documentation, and printer drivers visit the Xerox website at www.xerox.com.

Novell Distributed Print Services (NDPS) / Novell Enterprise Print Services (NEPS) are products built on Novell's printing architecture. Which allow administrators to take advantage of built-in printer intelligence to centrally manage network printing resources from anywhere on the network, improve network printing performance, and reduce the difficulty of network printing for end users.

The Xerox NDPS/NEPS Solution allows you to use Novell NDPS/NEPS with many of the latest Xerox printers. It includes administrative tools that snap-in to NWAdmin that enables users to easily configure and manage their network print services. It also has a set of NetWare Loadable modules that run on the NetWare server.

NetWare users have the ease of automatically creating a printer object in the NDS tree and automatic driver download capability, eliminating individual driver installation by downloading the driver as users connect to a printer. Network users can perform remote, up-to-the-minute status checks or define meaningful notifications for their Xerox network printers.

AS400 Raw TCP/IP Printing to Port 9100 (CRTDEVPRT)

This is the procedure to set up printing to a device from an AS/400 using the SNMP drivers.

This procedure is intended for users familiar with the AS/400 system, especially those experienced with printing in an AS/400 environment.

The AS/400 must run V4R5 of OS/400 so that the SNMP drivers are present (or V4R3/V4R4 with the most current PTFs installed).

The device must have port 9100 enabled.

Procedures to Enable Port 9100

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. Ensure the **[Enabled]** box is checked to enable Raw TCP/IP Printing.
9. Leave the **[TCP Port Number]** set to 9100 for Port 1.
10. Leave the **[Bidirectional]** and **[Maximum Connections]** settings at their default values.
11. Set the **[End of Job Timeout]** to the number of seconds to wait before processing a job without an End Of Job indicator.
12. Leave the **[PDL Switching]** Enabled box at its default value.
13. Click on the **[Apply]** button to accept the changes, or **[Undo]** to return the settings to their previous values, or **[Default All]** to enter printer defaults for all settings (recommended).
14. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you restart the device.

Create a Device Description

Create a device description from your AS400 terminal's command line.

1. Select the F-4 key to prompt the CRTDEVPRT command. Enter the following parameters:

   Device Description: Xeroxprinter

   Device Class: *lan

   Device Type: 3812

   Device Model: 1
2. Press **[Enter]** to continue, and enter the following parameters:

Lan Attachment: *IP

Port Number: 9100

Online at IPL: *yes

Font Identifier: 11

Form Feed *autocut

Note

For some versions of AS400, the default may match some of these parameters.

3. Leave all other parameters at the default value, press **[Enter]**, and enter the following parameters: Activation Timer: 170

   Inactivity Timer: *sec15

   Host Print Transform: *yes
4. Press **[Enter]** to continue, and enter the following parameter: Manufacturer Type and Model: *hp5si
5. Leave the remaining parameters set to their default values and press **[Enter]** to continue. Enter the following parameters: Remote Location: Enter the *IP address* of the printer.

   User defined options: *IBMSHRCNN

   System driver program: *IBMSNMPDRV
6. Leave all other options set to the default values and press **[Enter]**. A message indicates that you created the device Xerox printer.
7. Power on the device and start a print writer. Then place a spool file in the appropriate queue to test the printer.

AS400 Printing using LPR (CRTOUTQ) - Optional

Creating a remote queue (LPR) on the AS400

1. At the command line, issue CRTOUTQ and press F4, then F9 for additional parameters. The setup is as follows:

   Note

   ONLY CHANGE THE PARAMETERS IN BOLD.

   - Output queue: **queue name**
   - Library: **Library name**
   - Maximum spooled file size
   - Number of pages: ***NONE**
   - Starting time: **Time**
   - Ending time: **Time**
   - Order of files on queue: ***FIFO**
   - Remote system: ***INTNETADR**
   - Remote printer queue: **virtual printer name****

     Note

     The queue for ColorQube should be lp (lower case L and P).

   - Writers to autostart: **1**
   - Queue for writer messages: **QSYSOPR**
   - Library: ***LIBL**
   - Connection type: ***IP**
   - Destination type: ***OTHER**

- Transform SCS to ASCII: *__YES__
- Manufacturer type and model: *__IBM42011 ***SEE NOTE BELOW***__
- Workstation customizing object: __xxxxxxxx (leave as default)__
- Library: __xxxxxxxx (leave as default)__
- Internet address: __xx.xxx.x.xx (IP address of printer)__
- VM/MVS class: *__SAME__
- Forms control Buffer: *__SAME__
- Destination options: __XAIX__
- Text description
- Display any file: *__NO__
- Job separators: __0__
- Operator controlled: *__YES__
- Data Queue: *__NONE__
- Library:
- Authority to check: *__DTAAUT__

2. Press **[Enter]** to create.

   Note

   The Workstation Customizing Object is the file that was created in the Create a Device Description on page 5-28 step 2.

3. At this point, a spool file (document) should be able to be sent to the ColorQube device.

   Note

   If printing PCL, set this parameter to HPIIID, HP5Si (most of the HP drivers will work) and set Workstation customizing object as *none.
   If printing ASCII, set this parameter to *IBM42011 (which is the default).

UNIX

HP-UX Client (Version 10.x)

HP-UX workstations require specific installation steps to communicate with the machine. The machine is a BSD-style UNIX printer, whereas HP-UX is a System Vstyle UNIX. Use the correct case when entering commands; UNIX commands are case sensitive.

Note

All UNIX commands are case-sensitive, so enter the commands exactly as they are written.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure that the correct IP Address is being used for the machine. To verify this, print a Configuration Report from the device.

  At the Device

  - Press the **<Machine Status>** button on the device.
  - Touch the **[Machine Information]** tab.
  - Touch **[Information Pages]**.
  - Touch **[Configuration Report]**.
  - Touch **[Print]**, then touch **[Close]**.

The Configuration Report will print. Verify the addresses detailed under TCP/IP Settings.

- Ensure the machine is connected to the network with Ethernet cabling.
- Ensure you can PING the machine IP address from the UNIX workstation

Configure the Client

1. Add the machine hostname to the etc/hosts file on the HP-UX workstation or DNS server.
2. Ensure that you can ping the machine from the HP-UX workstation, using the hostname found in the **/etc/hosts file**.
3. Use either the **GUI** method or the **tty** Method as follows:

GUI Method

1. Open a command window from the desktop.
2. Type **[su]** to become super user.
3. Type **[sam]** to start the System Administrator Manager (SAM).
4. Select the **[Printers and Plotters]** icon.
5. Select **[lp]** spooler.
6. Select **[Printers and Plotters]**.
7. Select **[Actions: Add Remote Printer/Plotter...]**.
8. Enter the following information into the Add Remote Printer/Plotter form:
   - **[Printer Name: printer name]**. Where printer name is the name of the queue being created.
   - **[Remote System Name: hostname]**. Where hostname is the machine hostname from the /etc/hosts file.

- Select **[Remote Printer is on a BSD System]** and click **[OK]** to complete form.

9. Click **[Yes]** at the Configure HP UX Printers Subpanel screen. This screen may be obscured by Add Remote Printer/Plotter form.
10. Select **[File: Exit]**.
11. Select **[File: Exit Sam]**.
12. Type **[exit]** to exit super user mode.
13. Test the queue created. Type the command **[lp -d queuename /etc/hosts]**.

tty Method

Follow the steps below to use the HP System Administrator Manager (SAM) GUI (Graphical User Interface).

Note

Refer to the HP-UX documentation for additional information on using the System Administrator Manager (SAM).

1. Open a command window on the desktop. From the command prompt (#), enter the information below. Remember that UNIX commands are case-sensitive.
2. Type **[su]** to become super user
3. Type **[sh]** to run the Bourne shell.
4. Type **[lpshut]** to stop the print service.
5. Create the print queue by typing (on the same command line): **[lpadmin -pqueuename -v/dev/null -mrmodel -ocmrcmodel -osmrsmodel -ob3 -orc -ormhostname -orplp]**

   Where queuename is the name of the queue being created and hostname is the machine hostname from the /etc/hosts file.
6. Type **[lpsched]** to start the print service.
7. Type **[enable queuename]** to enable the queue to print to the machine.
8. Type **[accept queuename]** to the queue accepting jobs from the HP-UX workstation.
9. Type **[exit]** to exit the Bourne shell and then **[exit]** to exit super user mode.
10. Test the queue created. Type the command **[lp -d queuename /etc/hosts]**.
11. Verify that the job is printed at the device.

Solaris 2.x

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure that the correct IP Address is being used for the machine. To verify this, print a Configuration Report from the machine.

  At the Device

  a. Press the **<Machine Status>** button on the device.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.

The Configuration Report will print. Verify the addresses detailed under TCP/IP Settings.

To Configure your Solaris 2.x Client

- Ensure the machine is connected to the network with Ethernet cabling.
- Ensure you can PING the machine IP address from the UNIX workstation.
- Add the machine printer hostname to the etc/hosts file.

Note

Perform the following steps to create a machine print queue on a Solaris 2.x workstation using either the GUI or the TTY method.

GUI Method

1. Open a command window from the desktop.
2. Type **[su]** to become super user.
3. Type **[admintool]** to run the System Administrator Tool.
4. Select **[Browse:Printers]**.
5. Select **[Edit:Add:Access to Printer...]**.
6. Enter the following information into the Access to Remote Printer form:

   [Printer Name: queuename]. Where queuename is the name of the queue being created.

   [Print Server: hostname]. Where hostname is the machine hostname from the /etc/hosts file. Click **[OK]** to complete the form.
7. Type **[sh]** to run the Bourne shell.
8. Type **[lpadmin -p queuename -s hostname!lp]** to modify the remote queuename.
9. Type **[exit]** to exit the Bourne shell and **[exit]** to exit super user mode.
10. Test the queue created. Type the command **[lp -d queuename /etc/hosts]**.

tty Method

1. Type **[su]** to become super user.
2. Type **[sh]** to run the Bourne shell
3. Define the machine as a BSD style printer. Type **[lpsystem -t bsd hostname]**. Where hostname is the machine hostname from the /etc/hosts file.
4. Create the queue. Type **[lpadmin -p queuename -s hostname -T unknown -I any]**. Where queuename is the name of the queue being created.
5. Type **[exit]** to exit the Bourne shell and **[exit]** to exit super user mode.
6. Test the queue created. Type the command **[lp -d queuename /etc/hosts]**. Verify that the job prints at the device.

SCO UNIX Environment

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure that the correct IP Address is being used for the machine. To verify this, print a Configuration Report from the machine.

  At the Device

a. Press the **<Machine Status>** button on the device.
b. Touch the **[Machine Information]** tab.
c. Touch **[Information Pages]**.
d. Touch **[Configuration Report]**.
e. Touch **[Print]**, then touch **[Close]**.

The Configuration Report will print. Verify the addresses detailed under TCP/IP Settings.

Set up for a SCO UNIX Client

SCO UNIX workstations require specific installation steps to communicate with the machine. The machines are BSD style UNIX printers, whereas SCO is System V style UNIX.

- Ensure the machine is connected to the network with Ethernet cabling.
- Add the machine printer hostname to the /etc/hosts file on the SCO workstation.
- Ensure that you can Ping the machine from the SCO workstation, using the hostname found in the /etc/hosts file.

  Perform the following steps to create a machine print queue on a SCO UNIX workstation using either the GUI or the TTY method.

GUI Method

1. Log in as root.
2. From the Main Desktop, select icons: **[System Administration: Printers: Printer Manager]**.
3. Select **[Printer: Add Remote: UNIX...]**.
4. Enter the following information into the Add Remote UNIX Printer form:
5. Host: hostname (Where hostname is the machine hostname from the /etc/hosts file.)

   Printer: name of the queue being created, i.e: dc xxxq. Select **[OK]** to complete the form.
6. Select **[OK]** at the Message window.
7. Select **[Host:Exit]**.
8. Select **[File: Close this directory]**.
9. Select **[File: Close this directory]**.
10. Click **[Save]** at the warning confirmation window.
11. Type **[exit]** to log out of root account.
12. Open UNIX Window.

tty Method

1. Type **[su]** to become super user.
2. Type **[rlpconf]** to create a printer. Enter the following information:

   [Printer Name: queuename]

   [Remote Printer: r]

   [Hostname: hostname]

   If the information has been entered properly, type **[y]**.
3. Click **[Enter]** to accept default of a non-SCO remote printer.
4. Click **[Enter]** to accept default of non-default printer.
5. Click **[Enter]** to start process of adding queue.
6. Type **[q]** to quit the rlpconf program.

CUPS

The Common UNIX Printing System (CUPS) was created by Easy Software Products in 1998 as a modern replacement for the Berkeley Line Printer Daemon (LPD) and A T and T Line Printer (LP) system designed in the 1970s for printing text to line printers.

Currently available for downloading from a number of sources on the Internet, such as www.cups.org, CUPS is offered in both source code and binary distributions.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 2-5, so that the web user interface (Internet Services) can be accessed.
- Ensure that the DNS settings are configured.

Enable Port 9100 as additional support for HTTP (IPP) printing

1. At your Workstation, open the web browser and enter the *IP address* of the machine in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. Ensure the **[Enabled]** box is checked to enable Raw TCP/IP Printing.
9. Leave the **[TCP Port Number]** set to 9100 for Port 1. If two additional ports are available, click **[Default All]** to see if they set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
10. Leave the **[Bidirectional]** checkboxes and **[Maximum Connections]** settings at their default values.
11. Set the **[End of Job Timeout]** to the number of seconds to wait before processing a job without an End Of Job indicator.
12. Leave the **[PDL Switching]** Enabled box at its default value.
13. Click on the **[Apply]** button to accept the changes.
14. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.

    Note

    The settings are not applied until you restart the machine.

15. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
16. Click the **[Reboot Machine]** button and click **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

Installing CUPS on the UNIX workstation

The instructions for installing and building CUPS are contained in the CUPS Software Administrators Manual, written and copyrighted by Easy Software Products and available for downloading at: www.cups.org/documentation.php.

An Overview of the Common UNIX Printing System, Version 1.1, and a large amount of other descriptive documentation, is also available at this site.

The binary distribution of CUPS is available in tar format with installation and removal scripts, as well as in rpm and dpkg formats for RedHat and Debian versions of Linux. After logging into the workstation as root (su) and downloading the appropriate files to the root directory, the installation begins as follows:

Tar format:

After untarring the files, run the installation script with the ./cups.install (and press Enter).

RPM format:

rpm -e lpr

rpm -i cups-1.1-linux-M.m.n-intel.rpm (and press Enter).

Debian format:

dpkg -i cups-1.1-linux-M.m.n-intel.deb (and press Enter).

Note

RedHat Linux, versions 7.3 and newer, include CUPS support, so software downloading is unnecessary. CUPS is also the default printing system for Mandrake Linux.

Installing the Xerox PPD on the workstation

The Xerox PPD for CUPS is available on one of the CD-ROMs that came with your printer. From the CD-ROM, with root privileges copy the PPD into your CUPS ppd folder on your workstation. If you are unsure of the folder's location, use the Find command to locate the ppd's. An example of the location of the ppd.gz files in RedHat 8.1 is /usr/share/cups/model.

Adding the Xerox printer

1. Use the PS command to make sure that the CUPS daemon is running. The daemon can be restarted from Linux using the init.d script that was created when the CUPS RPM was installed. The command is > /etc/init.d/cups restart. A similar script or directory entry should have been created in System V and BSD. For the example of CUPS built and installed on a FreeBSD 4.2 machine from the source code, run cupsd from /usr/local/sbin. (cd /usr/local/sbin cupsd and press Enter).
2. Type http://localhost:631/admin into the address (URL) box of your web browser and press Enter.
3. For User ID, type root. For the requested password, type the root password.
4. Click **[Add Printer]** and follow the on screen prompts to add the printer to the CUPS printer list.

Printing with CUPS

CUPS supports the use of both the System V (lp) and Berkeley (lpr) printing commands.

Use the -d option with the lp command to print to a specific printer.

lp -dprinter filename (Enter)

Use the -P option with the lpr command to print to a specific printer.

lpr -Pprinter filename (Enter)

For complete information on CUPS printing capabilities, see the CUPS Software Users Manual available from www.cups.org/documentation.php.

6 Print Drivers

This chapter summarizes the print driver features and functions. You can use Internet Services to configure the Print Drivers.

Windows 2000/2003 Server

Xerox Printer Installer

This section provides instructions on how to install printer drivers manually. However, you can use Xerox Printer Installer to discover the printer and install drivers.

To use the Xerox Printer Installer locate the CentreWare Print and Fax Drivers CD-ROM delivered with your device and follow the instructions contained in the CentreWare Print and Fax Drivers Guide for Microsoft Windows.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Verify the device is configured with the correct IP Address, Subnet Mask, and Gateway Address information by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.
- Locate the CentreWare Print and Fax Drivers CD. (This was delivered in the CentreWare Network Services Pack with your device.) Review any README file contained with the printer drivers.

Windows Add Printer Wizard

1. At the Desktop, right-click the **[Network Neighborhood]** icon.
2. Select **[Properties]**.
3. Click on the **[Protocols]** tab.
4. Verify that the **[TCP/IP]** protocol has been loaded.
5. Select the **[Services]** tab and verify that **[Microsoft TCP/IP Printing]** is loaded. If this software is not present, install it using the documentation provided by Microsoft. Then return to the next step in this document.

Verify that Print Services for UNIX is loaded

1. From the **[Start]** menu, select **[Settings]**.
2. Select **[Control Panel]**.
3. Double-click **[Add/Remove Programs]**.
4. Select **[Add/Remove Windows Components]**.
5. Select **[Other Network File and Print Services]**.
6. Click **[Details]**.
7. Check the box to select **[Print Services for UNIX]**.

8. Click **[OK]**.
9. Click **[Next]**.
10. Close the **[Add/Remove Programs]** window.

Add the Printer

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]/[Printers and Faxes]**.
2. Double-click **[Add Printer]** and click on **[Next]**.
3. 16. Select **[Local Printer]** (Windows 2000) or **[Local Printer attached to this computer]** (Windows 2003) and deselect **[Automatically detect and install my Plug and Play printer]**.
4. Click **[Next]**.
5. Select **[Create a New Port]**.
6. Select **[LPR Port]** from the **Type of Port** drop-down menu and click **[Next]**.

   Note

   LPR Port is only available when Print Services for UNIX is installed.

7. Enter the **IP Address** of the printer.
8. Enter the printer name.
9. Click **[OK]**.
10. You will be prompted for a printer driver. Select **[Have Disk]** and click **[Browse]**. Locate the Drivers folder on the CD.
11. Select the required driver.
12. Click **[Open]** and then **[OK]**.
13. Select the model of your machine from the list. Click **[Next]**.
14. The **Name your Printer** screen appears. Enter a printer name and click **[Next]**.
15. The **Printer Sharing Screen** appears. If you will be sharing this printer with other clients select **[Share As]** (Windows 2000) or **[Share Name]** (Windows 2003) and enter a share name. Click **[Next]**.
16. Enter a name and comment if required. Click **[Next]**.
17. Select **[Yes]** to print a test page. Click **[Next]**
18. Click **[Finish]**. The printer driver will install.

Configure the Print Driver

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]**.
2. Right click on the printer icon and select **[Properties]**.
3. Click on the **[Advance]** tab, then click on **[Printing Defaults]**.
4. Select the settings you wish to set for the printer.

You have completed the installation of the printer driver on Windows 2000/2003 Server.

For further information on Configuring the Printer Driver and Installation, refer to the CentreWare Print Drivers Guide for Windows CD.

Windows 2000 Professional

Note
You can use CentreWare to configure the Print Driver in this environment.

Xerox Printer Installer

This section provides instructions on how to install printer drivers manually. However, you can use Xerox Printer Installer to discover the printer and install drivers.

To use the Xerox Printer Installer locate the CentreWare Print and Fax Drivers CD-ROM delivered with your device and follow the instructions contained in the CentreWare Print and Fax Drivers Guide for Microsoft Windows.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Verify the device is configured with the correct IP Address, Subnet Mask, and Gateway Address information by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.
- Locate the CentreWare Print and Fax Drivers CD. (This was delivered in the CentreWare Network Services Pack with your device.) Review any README file contained with the printer drivers.

To install printer drivers on Windows 2000 Professional choose one of the following options:

- Connect to an existing print queue already created on a network server
- Create a new print queue on the Windows 2000 Professional workstation

Connect to an Existing Print Queue

1. At the Windows 2000 Professional Desktop, right mouse click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click on the **[Local Area Connection]** icon.
4. Select **[Properties]**.
5. Verify that the Internet Protocol (TCP/IP) protocol has been loaded. If this software is not present, install it using the documentation provided by Microsoft. Then return to the next step in this document.

Add the Printer

1. From the **[Start]** menu, select **[Settings]**.
2. Select **[Printers]**.

3. Double-click **[Add Printer]** and click **[Next]**.
4. Verify that **[Network Printer]** is selected and click **[Next]**.
5. The Locate Your Printer screen will appear. Select the **[Type the Printer Name]** option or click **[Next]** to browse for a printer.
6. Enter the path to the printer or click **[Next]** to browse for the print queue created on your server.
7. Select the printer and click **[Next]**. Select **[Yes]** if you wish to make it the default printer. Click **[Next]**.
8. Click **[Finish]**. The printer driver will download to the Windows 2000 Professional workstation.
9. Once the printer driver has installed open an application on the workstation and print a test page to verify operation.

Create a New Print Queue

Go to the Windows 2000 Professional Workstation

1. At the Desktop, right click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click on the **[Local Area Connection]** icon and select **[Properties]**.
4. Verify that the [Internet Protocol (TCP/IP)] protocol has been loaded. If this software is not present, install it using the documentation provided by Microsoft. Then return to the next step in this document.

Verify that Print Services for UNIX is loaded

1. From the **[Start]** menu, select **[Settings]**.
2. Select **[Control Panel]**.
3. Double-click **[Add/Remove Programs]**.
4. Select **[Add/Remove Windows Components]**.
5. Select **[Other Network File and Print Services]**.
6. Click **[Details]**.
7. Check the box to select **[Print Services for UNIX]**.
8. Click **[OK]**.
9. Click **[Next]**.
10. Close the **[Add/Remove Programs]** window.

Add the Printer

1. From the **[Start]** menu, select **[Settings]** then **[Printers]**.
2. Double-click **[Add Printer]** and click **[Next]**.
3. Select **[Local Printer]** and deselect **[Automatically detect and install my Plug and Play printer]**.
4. Click **[Next]**.
5. Select **[Create a new port]** and choose **[LPR Port]** from the Type pull-down menu.
6. Click **[Next]**.
7. Enter the IP address of the printer.
8. Enter a name for the print queue and click **[OK]**.
9. You will be prompted for a printer driver. Select **[Have Disk]** and browse to the location of your printer drivers.
10. Select the **[.INF]** file then click **[Open]**.

11. The wizard will return you to the previous dialog. Verify the path and file name are correct and click **[OK]**.
12. Select the model that corresponds to your device and click **[Next]**.
13. The Name your Printer screen appears. Enter a printer name. Select **[Yes]** if you wish to make this the default printer, then click **[Next]**.
14. The Printer Sharing Screen appears. If you will be sharing this printer with other clients select the **[Share As]** button and enter a share name. Click **[Next]**.
15. Enter a location and comment (optional).
16. Select **[Yes]** to print a test page and verify that it prints at the device. Click **[Next]**.
17. Click **[Finish]**.

You have completed the installation of the printer driver on Windows 2000 Professional.

Configure the Print Driver

1. From the **[Start]** menu, select **[Control Panel]** and then **[Printers]**.
2. Right click on the printer icon and select **[Properties]**.
3. Click on the **[Configuration]** tab.
4. Change the settings you wish to set for the printer.
5. Click **[OK]**.

For further information on Configuring the Printer Driver and Installation, refer to the CentreWare Print Drivers Guide for Windows CD.

Windows XP

Note
You can use CentreWare to configure the Print Driver in this environment.

Xerox Printer Installer

This section provides instructions on how to install printer drivers manually. However, you can use Xerox Printer Installer to discover the printer and install drivers.

To use the Xerox Printer Installer locate the CentreWare Print and Fax Drivers CD-ROM delivered with your device and follow the instructions contained in the CentreWare Print and Fax Drivers Guide for Microsoft Windows.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Verify the device is configured with the correct IP Address, Subnet Mask, and Gateway Address information by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.
- Locate the CentreWare Print and Fax Drivers CD. (This was delivered in the CentreWare Network Services Pack with your device.) Review any README file contained with the printer drivers.

To install printer drivers on Windows XP choose one of the following options:

- Connect to an existing print queue already created on a network server
- Create a new print queue on the Windows XP workstation

Connect to an Existing Print Queue

1. At the Windows XP Workstation verify that the TCP/IP protocol stack is loaded: select **[Start]**, right-click the **[My Network Places]** icon, and select **[Properties]**.
2. Right-click on the **[Local Area Connection]** icon. Select **[Properties]**.
3. Verify that the Internet Protocol (TCP/IP) protocol has been loaded (it may be necessary to scroll down the list). If this software is not present, install it using the documentation provided by Microsoft. Then return to the next step in this document.
4. From the **[Start]** menu select **[Printers and Faxes]**. The Vista path is Start\Control Panel\Printer(s).
5. Select **[Add a Printer]**.
6. The Welcome Page appears. Click **[Next]**.
7. Verify that **[A network printer or a printer attached to another computer]** is selected and click **[Next]**.

8. The Specify a Printer screen will appear. Click **[Next]** to browse for the print queue created on your server, or if you know the name of the server and printer click **[Connect to this printer]** and enter the server and printer name details.
9. Select the printer and click **[Next]**.
10. Decide whether or not you want to make this printer your default printer, then click **[Next]**.
11. Click **[Finish]**. The printer will download to the Windows XP workstation.
12. Once the printer driver has installed, open an application on the workstation and print a test page to verify operation.

Configure the Print Driver

1. From the **[Start]** menu select **[Printers and Faxes]**. The Windows XP path is Start\Control Panel\Printers and Faxes.
2. Right click on the printer icon and select **[Properties]**. Use the available tabs to set the printing defaults. Additional settings may be accessed by clicking the **[Printing Preferences]** button on the General tab.

Create a New Print Queue on Windows XP

1. Obtain the Print Driver for your operating system.
2. Verify that Print Services for UNIX is loaded: from the **[Start]** menu, select **[Control Panel]**.
3. Double-click **[Add/Remove Programs]**.
4. Select **[Add/Remove Windows Components]**.
5. Scroll down until you see **[Other Network File and Print Services]**.
6. Click the **[Details]** button.
7. Check the box to add **[Print Services for UNIX]** if not already installed and click **[OK]**.
8. Click **[Next]**.

Add the Printer

1. From the **[Start]** menu select **[Printers and Faxes]**. The Vista path is Start\Control Panel\Printer(s).
2. Select **[Add a Printer]**, then **[Next]**.
3. Select **[Local Printer attached to this computer]**.
4. If already selected, Deselect **[Automatically detect and install my Plug and Play printer]**.
5. Click **[Next]**.
6. Select **[Create a new port]**.
7. Select **[LPR]** from the Type of Port pull down menu, then click **[Next]**.
8. Enter the IP Address of the printer.
9. Enter a name for the print queue and click **[OK]**.
10. You will be prompted for a printer driver. Select **[Have Disk]** and browse to the location of your printer drivers.
11. Select the **[.INF]** file then click **[Open]**.
12. When the Install from Disk screen appears, verify that the path and file name are correct, then click **[OK]**.
13. Select the model of your device from the list. Click **[Next]**.
14. The Name your Printer screen appears. Enter a printer name.
15. Decide whether or not you want to make this printer your default printer, then click **[Next]**.

16. The Printer Sharing Screen appears. If you will be sharing this printer with other clients select the **[Share Name]** button and enter a share name. Click **[Next]**.
17. Enter a location and comment in the **[Location and Comment screen]** (optional).
18. Select **[Yes]** to print a test page. Click **[Next]**
19. Click **[Finish]**. The printer driver will install. At the device and verify that the test page printed.

Configure the Print Driver

1. From the **[Start]** menu select **[Printers and Faxes]**. The Vista path is Start\Control Panel\Printer(s).
2. Right-click on the printer icon and select **[Properties]**.
3. Use the available tabs to set the printing defaults. Additional settings may be accessed by clicking the **[Printing Preferences]** button on the General tab.

You have completed the installation of the printer driver on Windows XP.

For further information on Configuring the Printer Driver and Installation, refer to the CentreWare Print Drivers Guide for Windows CD.

Windows Vista

Xerox Printer Installer

This section provides instructions on how to install printer drivers manually. However, you can use Xerox Printer Installer to discover the printer and install drivers.

To use the Xerox Printer Installer locate the CentreWare Print and Fax Drivers CD-ROM delivered with your device and follow the instructions contained in the CentreWare Print and Fax Drivers Guide for Microsoft Windows.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Verify the device is configured with the correct IP Address, Subnet Mask, and Gateway Address information by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.
- Locate the CentreWare Print and Fax Drivers CD. (This was delivered in the CentreWare Network Services Pack with your device.) Review any README file contained with the printer drivers.

To install printer drivers on Windows Vista choose one of the following options:

- Connect to an existing print queue already created on a network server
- Create a new print queue on the Windows Vista workstation

Connect to an Existing Print Queue

Note

You will need to know the server name where the print queue is located and the printer share name.

1. At your Workstation, click on **[Start]** then select **[Control Panel]**. Open the **[Printers]** folder.
2. Double-click on **[Add Printer]**.
3. Click **[A printer that is not attached to my computer (network printer)]**.
4. Click on **[Next]**.
5. The **Searching for network printer** screen will appear. Click on **[Next]**.
6. The **Specify a Printer** screen appears.
7. Click on **[Browse for a Printer]** and click on **[Next]**.
8. Select the server where the print queue is located and click the printer share name.
9. Click on **[OK]**.
10. Click on **[Yes]** to connect to the printer.

11. The **Printer installed screen** will appear. Select **[Print a Test Page]** to verify the printer is installed.
12. Select **[Make this my default Printer]** if required.
13. Click **[Next]**.
14. Click **[Finish]**.

Create a New Print Queue

- Ensure you have the CentreWare Print and Fax Drivers CD (delivered with your device).
- The device must be configured with a valid IP address or host name, subnet mask and gateway address.
- LPD (Line Printer Daemon) must be enabled on the device.

Verify that LPR Port Monitor is Loaded

1. Click **[Start]**, **[Control Panel]** and double-click **[Programs and Features]**.
2. Double-click **[Windows Features]**.
3. In the **[Turn Windows Features on and off]** window expand the **[Print Services]** menu.
4. Click on **[LPR Port Monitor]** to enable the service.
5. Click on **[OK]**. Your computer may need to restart.

Add the Printer

1. At your Workstation, click on **[Start]** then select **[Control Panel]**. Open the **[Printers]** folder.
2. Double-click on **[Add Printer]**.
3. Click **[A printer that is not attached to my computer (network printer)]**.
4. Click on **[Next]**.
5. Click **[Create a new port]**.
6. Select **[LPR Port]** from the **Type of Port** menu and click **[Next]**.
7. Enter the **IP Address** of the device.
8. Enter a name for the print queue.
9. Click on **[OK]**.
10. Click **[Have Disk]** and browse for the CentreWare Print and Drivers CD.
11. Select the required driver. Click **[Open]** and **[OK]**.
12. Select the printer model from the list.
13. Click on **[Next]**.
14. Select **[Print a test page]** to verify the printer is installed.
15. Select **[Make this my default]** if required.
16. Click on **[Finish]**.

Configure the Printer Driver

If your device has any installable options fitted then these should be set in the driver, for example, a High Capacity Feeder or a Finisher.

1. At your Workstation, click on **[Start]** then select **[Control Panel]**. Open the **[Printers]** folder.
2. Right click the appropriate printer icon and select **[Properties]**.
3. Click the **[Configuration]** tab.

4. Click **[Bi-Directional Setup]**. Bi-directional communication automatically updates the printer driver with the printer's installed options. The driver Printing Preferences will report information about the printer's operational status, active jobs, completed jobs and paper status. If you do not want to configure Bi-directional Setup go to step 7.
5. Click **[Automatic]** to have the driver automatically configure the IP address of the device or click **[Manual]** and enter the IP address or host name of the device.

   If you want to change the default SNMP settings, click **[SNMP Community Name]** and enter the required information.
6. Click on **[OK]**.
7. Click on the **[Installable Options]**.
8. If Bi-directional setup has not been enabled select the options that are installed on the device.
9. Click on **[OK]**.
10. Click on **[OK]** to close the Properties box.
11. Right click the printer within the Printers folder and select **[Printing Preferences]**.
12. Select any required default settings in the printer driver.

For further information on Configuring the Printer Driver and Installation, refer to the CentreWare Print Drivers Guide for Windows CD.

Apple Macintosh

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Verify the AppleTalk settings have been configured properly on the device by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.
- Locate the CentreWare Print and Fax Drivers CD. Review any README file contained with the printer drivers.

Install the Print Driver

View the Configuration Report and note the Name given to the device under AppleTalk Settings.

At the Macintosh Workstation

1. Load the CentreWare Print and Fax Drivers CD-ROM into your CD drive.
2. Open the CD and locate the **[Drivers]** folder.
3. Locate and open the **[Mac]** folder.

Instructions for 10.x (OS X)

At the Macintosh Workstation

1. Load the CentreWare Print and Fax Drivers CD-ROM into your CD drive.
2. Open the CD and select the required language if necessary.
3. Double-click to open the **[Drivers]** folder.
4. Double-click to open the **[Mac]** folder.
5. Double-click to open the folder containing the drivers for version 10.x.
6. Double-click to open the **[machine model.dmg]**.
7. Double-click to open the **[machine model.pkg]** file.
8. When the Welcome screen displays, click **[Continue]**.
9. Click **[Continue]**, then **[Agree]** to accept the Licence Agreement.
10. Select the required disk (if necessary) where you want to install the printer. Click **[Continue]**.
11. Click **[Install]**.
12. Click **[Close]**, and restart the workstation.
13. When the workstation has restarted, double click the hard drive icon.
14. Double-click the **[Applications]** icon.

15. Double-click the **[Utilities]** folder.
16. Double-click the **[Printer Setup Utility]** icon.
17. Double-click the **[Add]** button to add a new printer or click the **[Printers]** menu and click on **[Add Printer]**.
18. Select **[IP Printing]** from the top menu.
19. Select **[Internet Protocol Printing]** or **[LPD/LPR Printing]** from the next menu.
20. Enter the *IP address* of the printer.
21. Enter a name for the print queue. (You may leave this blank if you prefer).
22. Select **[Xerox]** from the **Printer Model** list.
23. Select your printer model from the **Model Name** list.
24. Click **[Add]**. The device will appear in the Printer List.
25. Select the printer and click the **[Show Info]** button.
26. Click **[Installable Options]**.
27. Select the options as installed on your device. If you want to use the Save Job for Reprint feature, ensure **Job Storage** is set to **[Installed]**.
28. Click **[Apply Changes]**.
29. Close the Printer Info box.
30. Print a document to verify that the printer is installed correctly.

View the Printer Utility on the CentreWare Print and Fax Services CD.

For further information on Configuring the Printer Driver and Installation, refer to the CentreWare Print Drivers Guide for Macintosh CD.

7 Authentication

Authentication Overview

The Authentication service can be enabled to prevent unauthorized use of installed device options. A System Administrator can configure the device, so that a user cannot access Color Copy, Workflow Scanning, E-mail, Internet Fax and Server Fax (when these features are installed on the device) unless the user has been authenticated.

There are five authentication options:

- **Authentication Off** (if available) Users can access any service without restriction.
- **Network Authentication** The System Administrator can select one of the following operating systems to provide network authentication:
  - Kerberos (Solaris)
  - Kerberos (Windows 2000/2003)
  - NDS (Novell)
  - SMB (Windows 2000/2003).
  - LDAP (Lightweight Directory Access Protocol).
- **Local Authentication** - With Local Authentication enabled, the System Administrator defines a passcode remotely, using a web browser, or locally at the device, allowing users to authenticate to the system and use restricted services.
- **Xerox Secure Access** - For information on this type of authentication, refer to Xerox Secure Access on page 21-1.
- **CAC (Common Access Card) / PIV (Personal Identification Verification)** - For information on this type of authentication, please refer to the CAC guide supplied with your device.

Authorization Overview

Once a user has been authenticated, the Authorization feature will validate the role of that user. A user can be defined as a System Administrator, an Accounting Administrator, or a general user. The Authorization feature verifies those areas of the device that a user is allowed to access, according to their role.

There are two options for Authorization:

- **Locally on the Device (Internal Database)** - refers to the database included on your device.
- **Remotely on a network** - refers to networked databases such as LDAP

The administrator can specify the services and device pathways on a device that require authentication. Services can be locked and/or hidden so that unauthorized users cannot use or see them. Pathways can be locked but not hidden.

Network Authentication

Network Authentication can be enabled to prevent unauthorized use of installed device options (for example, Machine Status Pathway, Job Status Pathway and Service Pathway such as Color Copy, Reprint Saved Jobs, Workflow Scanning, E-mail, Internet Fax and Fax).

Users of the device will be asked to provide a User Name and Password to be validated by the designated authenticated server. If this validation is successful, the options which were previously locked will be available for individual use.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the device is fully functional on the network.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional. This is required to access Internet Services to configure Network Authentication. Internet Services function is accessed through the embedded HTTP server on the device and allows System Administrators to configure Authentication settings by using an Internet browser.
- Ensure the Authentication Server to be used is functional on your network and refer to your manufacturer's documentation for instructions to complete this task.

Authentication Configuration Wizard

Admin Password

Initially when **Access Right** is selected, the **Authentication Configuration Wizard** will display. The first part of the **Authentication Configuration Wizard** is the **Device System Administrator Password** screen, you will be prompted to change the System Administrator Password. The System Administrator password is used to access Tools at the device user interface, and change settings via Internet Services.

For security reasons, if you have not changed your password, you must change your current System Administrator’s password.

1. Click on the **[Admin Password]** from the directory tree.
2. In the **New Admin Password** area, enter a password in the **[New Password]** box, and retype password in the **[Retype Password]** box.

WARNING

Do not forget this password, or you could be completely locked out of the system, requiring a service call.

3. Click on the **[Apply]** button to return to the **Authentication Configuration Wizard** page 1 of 3.

The following is an example steps of the Authentication Configuration Wizard

- **Step 1 of 3 - Authentication Configuration Wizard**

This screen explains the concepts of Authentication, Authorization, and Personalization.

- **Authentication** - Determines that the person who logs in has given the proper credentials and is known to the system.
- **Authorization** - Determines what an authenticated user can do, for example, the authenticated user has permission to use the Copy Service.
- **Personalization** - Adds personal settings for the authenticated user optimizing productivity, for example, automatically enter my email address to the From field.

- **Step 2 of 3 - Authentication Configuration Wizard**

  This page allows you to select the Authentication, Authorization and the Personalization methods.

- **Step 3 of 3 - Authentication Configuration Wizard**

  This page displays what configuration is Authenticated, Authorized and Personalized. This page is used for confirming or editing the authentication options that were established using the Authentication Configuration Wizard.

- Once the **Authentication Configuration Wizard** is completed, click on the **[Finish]** button.

Authentication Configuration

The following steps are written as subsequent use, assuming that the initial Authentication Configuration Wizard has previously been completed.

Authentication Configuration for Kerberos (Solaris)

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. Next, in the **Where is the Information Located?** area select **[Remotely on the Network]** form the drop down menu for **Device User Interface Authentication** and **Authorization**. Ensure that the **[Automatically retrieve user's e-mail address from LDAP]** checkbox under **Personalization** is checked, and click on the **[Save]** button to return to the **Authentication Configuration** page.
10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.
11. In the **Authentication Server** page, select **[Kerberos (Solaris)]** from the **Authentication Type** drop down menu.
12. In the **Default Key Distribution Center (Required)** area, enter details in the **[Realm]** field.
13. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
14. If IPv4 or IPv6 Address is selected, enter the **[IP Address]** and **[Port]** and **[Backup IP Address]** and **[Port]** details of the default **Default Key Distribution Centre (Required)**.
15. If Host Name is selected, enter the **[Host Name]** and **[Port]** and **[Backup Host Name]** and **[Port]** details of the **Default Key Distribution Centre (Required)**.

Note

Entering the IP address negates the need for name to IP resolution. Entering the NetBIOS Name or host name sends the name query request to either the WINS or DNS servers for resolution. Make sure the addresses of the WINS or DNS servers have already been set up for use with this device (under Connectivity/Protocols/Microsoft Networking or TCP/IP). Entering an IP Address or NetBIOS name can also be useful in allowing local network SMB name query broadcasts through a router, if so desired.

16. Enter details for up to 8 **[Alternate Key Distribution Centres (Optional)]** and backups, if required.
17. Click on the **[Save]** button to save the settings and return to the **Authentication Configuration** page.

Set Authentication to control access to individual Services

18. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
19. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
20. Click on the **[Save]** button and return to the **Authentication Configuration**.

Set Authentication to control access to individual Features

21. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
22. In the **Tools & Feature Access** page, under **Presets**, select either:
    - **Standard Access - Only Lock Tools**
    - **Open Access - Unlock All Tools and Features**
    - **Custom Access**

    If you select **[Custom Access]**, for each feature you can either select **[Unlocked]** or **[Locked]** from the drop down menu.
23. Click on the **[Apply]** button.
24. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
25. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Authentication Configuration for Kerberos (Windows 2000/2003)

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. Next, in the **Where is the Information Located?** area select **[Remotely on the Network]** from the drop down menu for **Device User Interface Authentication** and **Authorization**. Ensure that the **[Automatically retrieve user's e-mail address from LDAP]** checkbox under **Personalization** is checked, and click on the **[Save]** button to return to the **Authentication Configuration** page.
10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.

11. In the **Authentication Server** page, select **[Kerberos (Windows 2000/2003)]** from the **Authentication Type** drop down menu.
12. In the **Default Domain Controller (Required)** area, enter details in the **[Domain]** field.
13. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
14. If IPv4 or IPv6 Address is selected, enter the **[IP Address]** and **[Port]** and **[Backup IP Address]** and **[Port]** details of the default **Default Domain Controller**.
15. If Host Name is selected, enter the **[Host Name]** and **[Port]** and **[Backup Host Name]** and **[Port]** details of the **Default Domain Controller**.

    Note

    Entering the IP address negates the need for name to IP resolution. Entering the NetBIOS Name or host name sends the name query request to either the WINS or DNS servers for resolution. Make sure the addresses of the WINS or DNS servers have already been set up for use with this device (under Connectivity/Protocols/Microsoft Networking or TCP/IP). Entering an IP Address or NetBIOS name can also be useful in allowing local network SMB name query broadcasts through a router, if so desired.

16. Enter details for up to 8 **[Alternate Domain Controllers (Optional)]** and backups, if required.
17. Click on the **[Save]** button to save the settings and return to the **Authentication Configuration** page.

Set Authentication to control access to individual Services

18. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
19. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
20. Click on the **[Save]** button and return to the **Authentication Configuration** page.

Set Authentication to control access to individual Features

21. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
22. In the **Tools & Feature Access** page, under **Presets**, select either:
    - **Standard Access - Only Lock Tools**
    - **Open Access - Unlock All Tools and Features**
    - **Custom Access**

    If you select **[Custom Access]**, for each feature you can either select **[Unlocked]** or **[Locked]** from the drop down menu.
23. Click on the **[Apply]** button.
24. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
25. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Authentication Configuration for NDS (Novell)

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure the NetWare protocol is enabled on your device by printing a Configuration Report.

  At the Device

a. Press the **<Machine Status>** button.
b. Touch the **[Machine Information]** tab.
c. Touch **[Information Pages]**.
d. Touch **[Configuration Report]**.
e. Touch **[Print]**, then touch **[Close]**.

The Configuration Report will print. Verify the NetWare settings configured under Network Setup. NetWare should read Enabled.

For instructions on how to enable NetWare, refer to NetWare on page 5-26 of this guide.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. Next, in the **Where is the Information Located?** area select **[Remotely on the Network]** from the drop down menu for **Device User Interface Authentication** and **Authorization**. Ensure that the **[Automatically retrieve user's e-mail address from LDAP]** checkbox under **Personalization** is checked, and click on the **[Save]** button to return to the **Authentication Configuration** page.

   Note

   Make sure that the NetWare protocol has been enabled per the instructions contained in this guide in the Network Installation section. For NDS you will need to supply the NDS tree and context.

10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.
11. In the **Authentication Server** page, select **[NDS (Novell)]** from the **Authentication Type** drop down menu.
12. In the **Default Tree/Context (Required)** area, enter details in the **[NDS Tree]** and **[NDS Context]** fields.
13. In the **Alternate Tree/Context (Optional)**, enter details for up to 2 **[NDS Tree]** and **[NDS Context]** field, if required.
14. Click on the **[Save]** button to save the settings and return to the **Authentication Configuration** page.

Set Authentication to control access to individual Services

15. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
16. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
17. Click on the **[Save]** button and return to the **Authentication Configuration**.

Set Authentication to control access to individual Features

18. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
19. In the **Tools & Feature Access** page, under **Presets**, select either:
    – **Standard Access - Only Lock Tools**
    – **Open Access - Unlock All Tools and Features**

– **Custom Access**

If you select **[Custom Access]**, for each feature you can either select **[Unlocked]** or **[Locked]** from the drop down menu.

20. Click on the **[Apply]** button.
21. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
22. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003)

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. Next, in the **Where is the Information Located?** area select **[Remotely on the Network]** from the drop down menu for **Device User Interface Authentication** and **Authorization**. Ensure that the **[Automatically retrieve user's e-mail address from LDAP]** checkbox under **Personalization** is checked, and click on the **[Save]** button to return to the **Authentication Configuration** page.
10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.
11. In the **Authentication Server** page, select **[SMB (Windows 2000/2003)]** or **[SMB (Windows NT4)** from the **Authentication Type** drop down menu.
12. In the **Configuration (Required)** area, enter details in the **[Default Domain]** field.
13. Check the **Optional Information** box.
14. Select either **[IPv4 Address]** or **[Host Name]** radio button.
15. If IPv4 Address is selected, enter the **[IP Address]** and **[Port]** details in the required fields.
16. If Host Name is selected, enter the **[Host Name]** and **[Port]** details in the required fields.
17. In the Alternate Domains (Optional) area, enter details for up to 8 **[Alternate Domains (Optional)]**, if required.
18. Click on the **[Save]** button to save the settings and return to the **Authentication Configuration** page.

Set Authentication to control access to individual Services

19. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
20. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
21. Click on the **[Save]** button and return to the **Authentication Configuration**.

Set Authentication to control access to individual Features

22. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.

23. In the **Tools & Feature Access** page, under **Presets**, select either:
    - **Standard Access - Only Lock Tools**
    - **Open Access - Unlock All Tools and Features**
    - **Custom Access**

    If you select **[Custom Access]**, for each feature you can either select **[Unlocked]** or **[Locked]** from the drop down menu.
24. Click on the **[Apply]** button.
25. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
26. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Authentication Configuration for LDAP/LDAPS

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. Next, in the **Where is the Information Located?** area select **[Remotely on the Network]** from the drop down menu for **Device User Interface Authentication** and **Authorization**. Ensure that the **[Automatically retrieve user's e-mail address from LDAP]** checkbox under **Personalization** is checked, and click on the **[Save]** button to return to the **Authentication Configuration** page.

    Note

    LDAP can also simply be used as an Information (Personalization) server, supplying information to other Authentication servers being used on the network.
10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.
11. In the **Authentication Server** page, select **[LDAP]** from the **Authentication Type** drop down menu.
12. In the **Configuration** area, click on the **[LDAP Settings]** link.
13. Under the **[Server Information]** area, select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
14. If IPv4 or IPv6 Address is selected, enter the IP Address for **[Primary LDAP Server]** and **[Alternate LDAP Server]** or if Host Name is selected, enter the details for **[Primary LDAP Server]** and **[Alternate LDAP Server]**. The last field of the IP Address or Host Name should be used to supply the TCP port number of the LDAP process. The default is 389.
15. Specify the LDAP Server environment from the **[LDAP Server]** drop-down menu.
16. In the **Optional Information** area, enter the path to the LDAP objects to limit the LDAP search in the **[Search Directory Root]** area. The entry should be in base DN format (for instance, **ou=people, dc=xerox, dc=com**).

17. Select the required radio button under **[Login Credentials to Access LDAP Server]**. Quite often, to simply supply address information for E-mail, no login is required. For authentication purposes, however, select **[System]** to have the device log in to the LDAP server.
18. For Login Credentials, enter the device's Login Name and Password (if required) in the boxes provided.
19. If SSL (encryption) is desired, check the **[Enable SSL]** checkbox under **[SSL]**.
20. If SSL will be used, click the **[View Trusted SSL Certificates]** link to view secure certificates that have been uploaded to the device.

    Note

    If the LDAP Server is operating with encryption enabled, you will need the certificate from that server installed on this device.

21. Enter your required number for **[Maximum Number of Search Results]**. This is the maximum number of addresses that will appear which match the search criteria selected by the user.
22. Enter the required time to wait for **[Search Timeout]**. Alternatively, you may select **[Use LDAP Server Timeout]**.
23. If your primary LDAP server is connected to additional servers, select **[LDAP Referrals]** to include searches at the other servers.
24. Under the **[Perform Query on]** heading, select **[Surname and Given Name Fields]** to search for the user's last name (surname) and first name (given name). Alternatively, if you select **[Mapped Name Field]**, you can click on **[User Mappings]**, specify the base DN in **[Search Directory Root]**, enter a known common name in the **[Enter Name]** box, then click **[Search]**. The returned information for each attribute, configurable under **[Imported Heading]** will be shown in the column labelled Sample.
25. Click on the **[Apply]** button when done.

Set Authentication to control access to individual Services

26. Click on **[Setup]** in the directory link under **Access Rights** to display **Authentication Configuration** page, in the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
27. On the **Service Registration** screen, check the box to select the services you want to display on the machine touch interface.
28. Click on the **[Save]** button and return to the **Authentication Configuration**.

Set Authentication to control access to individual Features

29. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
30. In the **Tools & Feature Access** page, under **Presets**, select either:
    - **Standard Access - Only Lock Tools**
    - **Open Access - Unlock All Tools and Features**
    - **Custom Access**

    If you select **[Custom Access]**, for each feature you can either select **[Unlocked]** or **[Locked]** from the drop down menu.
31. Click on the **[Apply]** button.
32. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
33. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Configure Filters for LDAP

1. If you are continuing from Step 31 in the previous procedure **(Authentication Configuration for LDAP/ LDAPS)**, click the **[Custom Filters]** heading tab under the LDAP title.
2. **If you have already logged out of Internet Services, or closed your browser**, at a networked workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
3. Click the **[Properties]** tab.
4. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
5. Click on the **[Login]** button.
6. Click on the **[Connectivity]** link.
7. Click on the **[Protocol]** link.
8. Select **[LDAP]** in the directory tree.
9. Click on **[Custom Filters]** heading tab under the LDAP title.
10. On the **Custom Filters** screen, under **LDAP Authentication** area, check to select **[Append Base DN]** box. When enabled, this will specify the distinguished name(s) that will lead to the entry in the LDAP directory under which all users and groups will be retrieved. Distinguished name is a unique name for an entry in your LDAP directory. For example: cn=USERID, o=xerox, c=us.

    Note

    Many UNIX/Linux LDAP servers require this attribute to be set and is used frequently when **Login Credentials to Access LDAP Server** is set to **[Authenticated User]**.

11. Select one or both of the **[Enable Custom Filter]** boxes, for the type of filter that you wish to apply.
12. For the **[E-mail Address Book filter]**, in the box provided, type in the LDAP search string (filter) that you wish to apply. The filter defines a series of conditions that the LDAP search must fulfill in order to return the information you seek. The form of the typed search string (filter) is LDAP objects placed inside parenthesis. For example, to find all users that have an E-Mail attribute (mail enabled), type (objectClass=user) (mail=*). If you are not familiar with LDAP search strings, use an Internet browser search to find examples.
13. For the **[User ID Query Filter]**, in the box provided, type in the LDAP search string (filter) that you wish to apply. The filter defines a series of conditions that the LDAP search must fulfill in order to return the information you seek. The form of the typed search string (filter) is LDAP attributes placed inside parenthesis. For example, to find the user with a sAMAccountName of Bob, type (objectClass=user) (sAMAccountName=Bob). If you are not familiar with LDAP search strings, use an Internet browser search to find examples.
14. Click on the **[Apply]** button when done.
15. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Configure Contexts for LDAP

Contexts are used with the Authentication feature. The administrator can configure the device to automatically add an authentication context to the Login Name provided by the user.

1. If you are continuing from Step 31 in the previous procedure **(Authentication Configuration for LDAP/ LDAPS)**, click on **[Contexts]** heading tab under the LDAP title.
2. If you have already logged out of Internet Services, or closed your browser, at a networked workstation, open the web browser and enter the *IP address* of the device in the Address or Location field. Press **[Enter]**.
3. Click the **[Properties]** tab.

4. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
5. Click on the **[Login]** button.
6. Click on the **[Connectivity]** link.
7. Click on the **[Protocol]** link.
8. Select **[LDAP]** in the directory tree.
9. Click on **[Contexts]** heading tab under the LDAP title.
10. Enter details in the **[Default Login Context]** box provided.
11. Click on the **[Apply]** button.
12. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
13. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Configure Authorization Access (by groups) for LDAP

LDAP server user groups can be used to control access to certain areas of the Xerox device. For example, the LDAP server may contain a group of users called "Admin." You can configure the "Admin" group on the device so that the members of that group will have administrator access to the device. When a user logs in at the device with their network authentication account, the device performs an LDAP look-up to determine if the user is a member of any groups. If the LDAP server confirms that the user is a member of the "Admin" group, the user will have administrator access to the device.

1. If you are continuing from Step 31 in the previous procedure **(Authentication Configuration for LDAP/ LDAPS)**, click on **[Authorization Access]** heading tab under the LDAP title.
2. If you have already logged out of Internet Services, or closed your browser, at a networked workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
3. Click the **[Properties]** tab.
4. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
5. Click on the **[Login]** button.
6. Click on the **[Connectivity]** link.
7. Click on the **[Protocol]** link.
8. Select **[LDAP]** in the directory tree, then click on **[Authorization Access]** heading tab under the LDAP title.
9. Select the **[User Roles]** tab.
10. In the System Administrator Access **[Access Group]** box, enter the name of a group, defined at the LDAP server, that you want to provide with System Administrator access to the device.
11. In the Accounting Administrator Access **[Access Group]** box, enter the name of a group, defined at the LDAP server, that you want to provide with accounting administrator access to the device.
12. To verify either group, enter a name of one of the members of the LDAP server group in the **[User Name box]**, then click on the **[Test]** button.
13. When done, click on the **[Apply]** button.
14. Select the **[Device Access]** tab.
15. In the **Services Pathway [Access Group]** box, enter the name of a group, defined at the LDAP server, that you want to provide with Service access to the device.
16. Repeat the process for **Job Status Pathway** and **Machine Status Pathway**.
17. To verify any of these groups, enter a name of one of the members of the LDAP server groups in the **[Enter User Name]** box, then click on the **[Test]** button.
18. When done, click on the **[Apply]** button.

19. Select the **[Service Access]** tab, then enter the names of LDAP groups, as required in the **Access Group** box, to allow access to individual device services.
20. Verify each group by entering a group user in the **Enter User Name** box, and click on the **[Test]** button.
21. When done, click on the **[Apply]**.
22. Select the **[Feature Access]** tab, then in the Color Copying **[Access Group]** box, enter the name of a group, defined at the LDAP server, that you want to provide with Color Copying access to the device.
23. To verify the groups, enter a name of one of the members of the LDAP server group in the **Enter User Name** box, then click on the **[Test]** button.
24. When done, click on the **[Apply]** button.
25. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Local Authentication

With Local Authentication enabled, the System Administrator defines passwords via a web browser, or locally at the device, for users to use to authenticate to the system and use restricted services.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. Next, in the **Where is the Information Located?** area select **[Locally on the Device (Internal Database)]** from the drop down menu for **Device User Interface Authentication** and **Authorization**, click on the **[Save]** button to return to the **Authentication Configuration** page.
10. In the **Current Configuration** area, click on the **[View]** button for **Local User Information Database**.
11. Click on the **[Add New User]** button, in the **User Identification** area, enter details of the new user in the **[User Name]**, **[Friendly Name]**, **[Password]** and **[Retype Password]** fields.
12. In the **[User Role]** area, select either one of the three radio button.
13. Click on the **[Add New User]** button to add the user, then press the **[Close]** button to return to the **Authentication Configuration** page.

    Note

    You can also Edit user credentials, as well as Delete users, from the **User Information Database** screen.

Set Authentication to control access to individual Services

14. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
15. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
16. Click on the **[Save]** button and return to the **Authentication Configuration**.

Set Authentication to control access to individual Features

17. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.

18. In the **Tools & Feature Access** page, under **Presets**, select either:
    - **Standard Access - Only Lock Tools**
    - **Open Access - Unlock All Tools and Features**
    - **Custom Access**

    If you select **[Custom Access]**, for each feature you can either select **[Unlocked]** or **[Locked]** from the drop down menu.
19. Click on the **[Apply]** button.
20. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
21. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Adding User Accounts at the Device

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Security Settings]**.
5. Touch **[User / Administrator Accounts]**.
6. Read the on screen instructions to configure a **User Account**.
7. Touch **[Configure Account]**, touch **[User Account]**, enter a Passcode of 1 - 9 digits, and touch **[Save Account]**.
8. Touch **[Close]**.
9. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

802.1X Authentication

The device supports 802.1X authentication based on the Extensible Application Protocol (EAP). 802.1X can be enabled for devices connected through both wired and wireless Ethernet networks. As described here, the 802.1X configuration is used to authenticate the device, rather than individual users. After the device has been authenticated, it will be accessible to users on the network.

The administrator can configure the device to use one EAP type. EAP types currently supported on the device are:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Create a user name and password on your authentication server which will be used to authenticate the Xerox device.
- Ensure your 802.1X authentication server and authentication switch are available on the network.

Enable 802.1X

At the Device:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[Advanced Settings]**.
6. At the Warning screen, touch **[Continue]**.
7. Touch **[802.1X]**.
8. Touch **[Enable]**.
9. Select the Authentication Method (EAP type) used on your network by touching the **[Authentication Method]**.
10. Touch **[Username]**.
11. Enter the user name required by your authentication switch and server.
12. Touch **[Save]**, and **[Save]** again.
13. Touch **[Close]**.
14. Touch **[Password]**.
15. The network controller will now reset taking the device offline for several minutes.
16. When the device comes back online, if the Tools screen is still displayed, with a message indicating that you are still logged in as Administrator, press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

Configure 802.1X with Internet Services

In addition to enabling 802.1X at the device, 802.1X can be configured with Internet Services (the embedded HTTP server running on the device). Make sure that the HTTP and TCP/IP protocols are properly configured for your network before attempting to use your web browser to communicate with the device's HTTP server.

Note

Some ports in an 802.1X environment may not be open, preventing Internet Services screens from being displayed. If this is the case, enable and configure 802.1X first at the device as previously stated in this section, then use Internet Services to modify settings as required and stated below.

Note

802.1X Port Based Network Access Control is used to ensure that devices that are connected to the network have the proper authorization. The 802.1X configuration is used to authenticate the multifunction device rather than an individual user. After the device has been authenticated, it will be accessible to users on the network.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Select **[802.1X]** in the directory tree.

7. Check the **[Enable 802.1X]** box.
8. Select the required **[EAP]** type from the **[Authentication Method]** drop down menu.
9. Enter the **[User Name (Device Name)]** and **[Password]** required by your authentication switch and server.
10. Click on the **[Apply]** button.
11. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
12. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Xerox Secure Access

Xerox Secure Access enables customers to leverage Xerox Partner Solutions to provide user authentication with an optional card reader. Users can access the features available at the device once they have been authenticated.

System Administrators can configure the device so that users must be authenticated and authorized before they can access specific services or areas. Xerox Secure Access provides a means of authenticating users via an authentication server and optional card reader.

Secure Access and Accounting

Secure Access can be enabled with the Network Accounting, Xerox Standard Accounting features for accounting purposes. When Network Accounting is enabled, the device can be configured to automatically obtain accounting data from the Network Accounting server when the user is authenticated.

Note

Secure Access cannot be enabled at the same time as Foreign Device Interface.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure that the device is fully functional on the network. TCP/IP and HTTP protocols must be configured so that Internet Services can be accessed.
- Ensure that the Xerox Partner authentication solution (Secure Access Server, Controller, and Card Reader) is installed and communicating with the device. Follow the installation instructions from the manufacturer of the authentication solution to correctly set the devices up. Make sure to securely mount any external user authenticating devices to the device.
- Ensure that SSL (Secure Sockets Layer) is configured on the device. The Xerox Partner authentication solution communicates with the device via HTTPS.
- (Optional) Ensure that Network Accounting is configured if you want the device to send user account information to a Network Accounting server. For instructions, refer to the Network Accounting section of this guide.
- You may also need another Authentication Server (running LDAP in an ADS environment, for example) to communicate with the Secure Access Server providing that server with user credentialing information.

A second Authentication Server will be necessary for web user interface Authentication, if this feature is additionally desired.

- You will need to configure LDAP communications on the device as stated in the LDAP/LDAPS topic in the Authentication section of this guide.

Configure Authentication

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page displays, in the **Current Configuration** area, click on the **[Edit Methods]** button for **Authentication**.
9. Next, in the **Where is the Information Located?** area select **[Xerox Secure Access]** form the drop down menu for **Device User Interface Authentication**.
10. Select your required option from the **[Web User Interface Authentication]** drop down menu. When a user attempts to access Internet Services they are prompted to enter their login information. The option selected from the web user interface Authentication menu defines how the device will validate the user's rights to access Internet Services. This is required because if the user normally authenticates at the device with a card reader, there would be no method for the device to authenticate users who access Internet Services from their workstations.
    - Select **[Locally on the Device]** to validate users listed in the Local User Information Database. This option requires you to configure accounts in the Local User Information Database.
    - Select **[Remotely on the Network]** to validate users via an Authentication Server. This option requires you to have a server that will provide authentication of user login details. Authentication via Kerberos (Solaris, Windows 2000), NDS (Novell), SMB (Windows NT4/2000) or LDAP is supported.
11. Select required method from the **[Authorization]** drop down menu. The card reader and Authentication Solution authenticates (validates) the user. The Authorization method determines which areas of the device a user is allowed to access. There are two options:
    - Select **[Locally on the Device]**: if you want the device to check the Local User Information Database for levels of authorization.
    - Select **[Remotely on the Network]**: if you want to use an LDAP server to determine levels of authorization.

    If you selected Remotely on the Network (from the Location of Access Rights box), configure LDAP communications as stated in the Configure Authentication for LDAP/LDAPS in the Authentication section of this guide.
12. Check the checkbox next to **[Automatically retrieve user's e-mail address from LDAP]** under **Personalization** is checked if you want to set the From address to the logged in user's e-mail address, when they log in via Secure Access.
13. Click on the **[Save]** button to return to the **Authentication Configuration** page.
14. In the **Current Configuration** area, click on the **[Configure]** button for **Device User Interface Authentication - Xerox Secure Access**.
15. Click on the **[Manually Configure]** button

16. In the **Server Communication** area, select either **[IPv4 Address]** or **[Hostname]**.
17. Enter details in the **IP Address** and **Port** or **Host Name** and **Port** fields.
18. Enter the details in the **[Path]** field.
19. Under the **Device Log In Methods** heading, select **[Xerox Secure Access Device Only (e.g., Swipe Cards]** if you wish to allow the user to enter their swipe card at the UI.
    Select **[Xerox Secure Access Device + alternate on-screen authentication method]** if this option should not be allowed.
    When the second option is enabled, a button labelled "Alternate Login" is displayed on the "Instructional Blocking Window" providing users with an alternate method to log in. For example, this feature can be enabled for users who are unable to use their swipe card. When the alternate button is selected, the remote server presents a series of log in screens on the local user interface. The remote server is still responsible for authenticating the user. All other Xerox Secure Access options are supported with this setting.
20. Under the **Accounting Information** heading, note that this item will be grayed out if Network Accounting is not enabled. If accounting is enabled, select **[Automatically apply Accounting Codes from the server]**, if the Secure Access Server has been configured to return the accounting User ID and Account ID login. If you want the user to enter these values at the local user interface during login, select **[User must manually enter accounting codes at the device]**.
21. Under the **Device Instructional Blocking Window** heading, enter text in the **[Window Title]** and **[Instructional Text]** boxes to create the prompt that will be displayed on the device's user interface informing users how to authenticate themselves at the device.

    Note

    If the Title and Prompt have been configured on the Secure Access Server, then this information will override the Title and Prompt text entered here.

22. Click **[Save]** when done.

Enable Web User Interface Authentication

A second, networked Authentication Server will be necessary for web user interface Authentication, if this feature is additionally desired. Full instructions for configuring network authentication, using Kerberos, NDS, SMB, and LDAP/LDAPS are contained in the Network Authentication section of this guide.

The path to the Authentication Server configuration screen is:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page displays, Click on the **[Edit Methods]** button for **Authentication** in the **Current Configuration** area.
9. In the **Where is the information located?** area, select **[Xerox Secure Access]** from the drop down menu for **Device User Interface Authentication**, and select **[Remotely on the Network]** from the drop down menu for **Web User Interface Authentication** and **Authorization**. Click on the **[Save]** button to return to the **Authentication Configuration** page.

10. In the **Current Configuration** area, click on the **[Configure]** or **[Edit]** button for **Web User Interface Authentication**.
11. Follow the instructions to select the required Authentication Type.
    - See Authentication Configuration for Kerberos (Solaris) on page 7-3.
    - See Authentication Configuration for Kerberos (Windows 2000/2003) on page 7-4.
    - See Authentication Configuration for NDS (Novell) on page 7-5.
    - See Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003) on page 7-7.
    - See Authentication Configuration for LDAP/LDAPS on page 7-8.

    When you have configured the required Authentication Type, click on the **[Save]** button to return to the **Authentication Configuration** page.

Configure your LDAP Server

Configure LDAP communications on the device as stated in the LDAP/LDAPS topic, see Authentication Configuration for LDAP/LDAPS on page 7-8.

Set Authentication to control access to individual Services

12. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
13. On the **Service Registration** screen, check the boxes to select the services you want to display on the machine touch interface.
14. Click on the **[Save]** button and return to the **Authentication Configuration**.

Set Authentication to control access to individual Features

15. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
16. In the **Tools & Feature Access** page, under **Presets**, select either:
    - **Standard Access - Only Lock Tools**
    - **Open Access - Unlock All Tools and Features**
    - **Custom Access**

    If you select **[Custom Access]**, for each feature you can either select **[Unlocked]** or **[Locked]** from the drop down menu.
17. Click on the **[Apply]** button.
18. Click on the **[OK]** button, when you see the window that says **"Properties have been successfully modified"**.
19. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Using Secure Access

1. Read the device's user interface prompt to determine what needs to be done to be authenticated at the device. Authentication methods include swiping a card, placing a proximity card near the reader, or entering a user ID or PIN (personal identification number).
2. If the device requests further information such as accounting details, enter this information at the user interface.
3. The device will confirm successful authentication allowing access to previously locked system features.

4. When finished using system features, press the **[Clear All]** button on the device's keypad to close your account.

8 Security

This chapter describes how to configure the following Security features for the device:

Security @ Xerox

For the latest information on securely installing, setting up and operating your device see the Xerox Security Information website located at www.xerox.com/security.

User Data Encryption

User Data Encryption ensures that any scan/print user or job sensitive data that resides on the device is secure.

User Data Encryption is automatically **enabled** on the device and no further configuration is required by the administrator.

If the hard disk is removed from the network controller then the encrypted data remains protected because the encryption key is not stored on the network controller hard drive.

Note

Changing the User Data Encryption setting will reboot the Network Controller. This may result in a loss of user data and will interrupt or delete current jobs on the device.

To Disable User Data Encryption:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Select **[User Data Encryption]** in the directory tree.
7. Under **[User Data Encryption Enablement]** select **[Disabled]**, click on the **[Apply]** button.

   Note

   Changing the User Data Encryption setting will reboot the Network Controller. This may result in a loss of user data and will interrupt or delete current jobs on the device.

User Information Database

The User Information Database allows you to add new users to the database, once added they can be deleted from the database and information of the user can also be edited.

Password Settings allows you to change password rules.

Note

If the Password rules are changed, old passwords are NOT AFFECTED by the new rules.

Setup

To add a new user to the database:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[User Information Database]** link.
7. Select **[Setup]** in the directory tree.
8. On the **User Information Database** page, click on the **[Add New User]** button.
9. On the **Add New User** page, in the **User Identification** area, enter the relevant details in all fields.
10. In the **User Role** area, select either one of the user role, and click on the **[Add New User]** button.

To Edit a User on the Database:

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.

6. Click on the **[User Information Database]** link.
7. Select **[Setup]** in the directory tree.
8. On the **User Information Database** page, click on the **[Edit]** link next to the user you want to edit.
9. On the **Edit User** page, edit any relevant field, and click on the **[Edit User]** button.

Password Settings

Use this page to set or change the password rules. This page is only available to users who are System Administrators

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[User Information Database]** link.
7. Select **[Password Settings]** in the directory tree.
8. On the **Password Settings** page, in the **Password Rules** area, enter details in the **[Minimum Length]** and **[Maximum Length]** field.
9. Check to select either or all options:
   - Cannot contain **"Friendly Name"**.
   - Cannot contain **"User Name"**.
   - Must contain **"at least 1 number"**.
10. Click on the **[Save]** button.

Admin Password

There are two options on this page:

- **New Password** - this option allows you to change password
- **Reset Policy** - this option allows you to either enable or disable Password Reset.

New Password

This page is part of the **Authentication Configuration Wizard**. It is also accessible from the Authentication Configuration page.

> Note
> The first time that Authentication Configuration is selected the **Device System Administrator Password** page appears. Use this page to change the default password before proceeding to any authentication configuration settings.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.

5. Click on the **[Security]** link.
6. Select **[Admin Password]** in the directory tree.
7. Ensure **New Password** tab is highlighted on the top of the screen.
8. Enter detail in the **[New Password]** and **[Retype New Password]** fields.
9. Click on the **[Apply]** button.

Note

The user name **"admin"** is reserved for the Device System Administrator Account.
Do NOT use the username **"admin"** for any local or network accounts on the device.

Reset Policy

This page allows you to enable or disable the Password Reset Policy.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Select **[Admin Password]** in the directory tree.
7. Ensure **Reset Policy** tab is highlighted on the top of the screen.
8. In the **Password Reset Policy** select either:
   - **Enable Password Reset**
   - **Disable Password Reset**
9. Click on the **[Apply]** button.

Note

This policy will be followed if the admin password is forgotten!
If Enabled, the password can be reset to the Factory Default using directions available from Xerox Support.
If Disabled, a **chargeable service call** would be required if the password is forgotten.

IP Filtering

The IP Filtering security feature provides the ability to prevent unauthorized network access based on IP address and/or port number filtering rules set by the System Administrator using Internet Services.

Authorized users will be able to create IP Address filtering rules.

Authorized users can enter a list of addresses that shall be allowed to access the device, and/or a list of addresses that are not allowed to access the device.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address or Location field. Press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.

6. Select **[IP Filtering]** in the directory tree.

Defining IP Filtering with the Define IP Filter Rule dialog

7. Click on the **[Add]** button to display the **Add IP Filter Rule** page.
8. From the **[Protocol]** drop-down list, select the protocol (All, TCP, UDP or ICMP) that the rule will apply to.
9. From the **[Action]** drop-down list, select how you wish IP Filtering to handle the incoming packet.
10. From the **[Move This Rule To]** drop-down list, select either End of List or Beginning of List for the location of this rule. Note that rule order is important in IP Filtering because rules can negate each other if placed in an incorrect order.
11. Enter the **[Source IP Address]** to which this rule will apply.
12. Enter a number for the **[Source IP Mask]** to which this rule will apply. The allowable range of 0 to 32 corresponds to the 32 bit binary number comprising IP addresses. A number of 8, for example, represents a Class A address (mask of 255, 0, 0, 0). The number 16 represents a Class B address (mask of 255, 255, 0, 0). The number 24 represents a Class C address (mask of 255, 255, 255, 0).
13. **[Source Port]**: This selection is only available when the Protocol has been set to TCP. Enter the originating port (if applicable) that the rule has been created to handle. If the incoming packet did not originate from this source port, the rule will not be applied.
14. **[Destination Port]**: This selection is only available when the protocol is set to TCP or UDP. Enter the destination port that the rule has been created to handle. If the incoming packet was not sent to this port, the rule will not be applied.
15. **[ICMP Message]**: This selection is only available when the protocol is set to ICMP. Select which ICMP Message the rule is meant to handle.
16. Click on the **[Apply]** button to accept the changes or on the **[Cancel]** button to exit the window without saving changes.

    Note

    The settings are not applied until you restart the device.

Audit Log

Audit Log is a log that tracks access and attempted access to the server. With TCP/IP and HTTP-based processes running on the server, exposure to access attacks, eavesdropping, file tampering, service disruption, and identity (password) theft is significantly increased. The Audit Log, regularly reviewed by the System Administrator, often with the aid of third party analyzing tools, helps to assess attempted server security breaches, identify actual breaches, and prevent future breaches. Access to the log's data is protected by enabling SSL (Secure Sockets Layer) protocols. The audit log, and its associated data protected by strong SSL encryption, helps to meet the Controlled Access Protection (Class C2) criteria, set by the United States Department of Defense. To enable this feature, perform the following steps.

IMPORTANT: Audit Log cannot be enabled until SSL (Secure Sockets Layer) is enabled on the device. To enable SSL on a device, the device needs to have a Server Certificate. For instructions to set up a Server Certificate, see Machine Digital Certificate Management on page 8-9.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.

5. Click on the **[Security]** link.
6. Select **[Audit Log]** in the directory tree. Note that you must enable SSL before enabling Audit Log.
7. Click on the **[Enabled]** checkbox for the **Audit Log**.
8. Click on the **[Apply]** button.
9. Click on the **[Save]** button to save the log as a text file.
10. Right-click on the **[Download Log]** link and select **[Save Target As..]** to download file.
11. The Audit Log is saved as **[Auditfile.txt.gz]**. This is a text file compressed as a GZIP file.
12. Open the **[Auditfile.txt.gz]** compressed file.
13. The Auditfile.text is a raw text file. To view the Audit Log as tab-delimited text, open the Auditfile.txt document in an application that can import text as a tab-delimited document, such as Microsoft® Excel.

View the Audit Log File

Event ID

A unique value that identifies the entry. The following list shows the ID number allocated to each type of activity displayed in the Audit Log:

1 = System start-up

2 = System shutdown

3 = On Demand Image Overwrite started

4 = On Demand Image Overwrite complete

5 = Print job

6 = Network Scan job

7 = Server Fax job

8 = IFAX

9 = E-mail job

10 = Audit Log Disabled

11 = Audit Log Enabled

12 = Copy

13 = Embedded Fax

14 = Print/Fax driver LAN Fax job

15 = Data Encryption

16 = Scheduled ODIOD Standard started

17 = Scheduled ODIO Standard complete

18 = Scheduled ODIO Full started

19 = Scheduled ODIO Full complete

20 = Scan to Mailbox job

21 = Delete File/Dir (CPSR)

22 = USB

23 = Scan to Home

24 = System Configuration Data Changes

Event Description

The Audit Log contains a maximum list of the last 15,000 activities on the device. The activities that are displayed include:

- System start up and shutdowns.
- On demand image overwrites completed.
- Jobs completed.
- Embedded Fax jobs.
- Store Files jobs.
- Accounting information.
- Workflow Scanning jobs - one scan to file audit log entry is recorded for each network destination within the scan job.
- Server Fax jobs - one audit log entry is recorded for each job.
- E-mail jobs - one audit log entry is recorded for each SMTP recipient within the job.

Completion Status

The Completion Status column shows the status of jobs and has the following values:

- comp-normal - the job completed correctly.
- comp-deleted - the job was deleted.
- comp-terminated - the job was cancelled.

Identify the PC or User

To record the user's name in the Audit Log, Network Authentication must be configured on the Xerox device.

IIO Status

If IIO (Immediate Image Overwrite) is enabled, this column will show the status of overwrites completed on each job.

Entry Data

This column contains any additional data that is recorded for an Audit Log entry, for example:

- Machine name.
- Job name.
- Username.
- Accounting Account ID (when Network Accounting is enabled).

Machine Digital Certificate Management

Machine Digital Certificates provide keys for encryption/decryption of data, it ensures the data is not tampered with and to validate the source of data.

A Digital Certificate is like an 'Electronic Driver's Licence'. It contains the following:

- Name of whom the Certificate is Issued to.
- Serial Number.
- Expiration Date.
- Name of the Certificate Authority that Issued the Certificate.
- A Public Key.
- A Digital Signature of the Key from a Certificate Authority.
- Country Code.

Other optional information it can contain is:

- State/Province Name.
- Locality Name.
- Organization Name.
- Organization Unit.
- E-mail Address.

The device can be configured for secure access with the SSL (Secure Socket Layer) protocol via Digital Certificates. The enablement of SSL provides encryption for all workflows where the device is used as a HTTPS server.

Workflows include:

- Administration of the device via Internet Services
- Printing via Internet Services
- Printing via IPP
- Scan Template Management
- Workflow Scanning via HTTPS
- Administration of Network Accounting

The device exports the signed certificate to the client to establish an SSL/HTTPS connection.

There are two options available to obtain a server certificate for the device:

- Have the device create a Self Signed Certificate
- Create a request to have a Certificate Authority sign a certificate that can be uploaded to the device.

A self-signed certificate means that the device signs its own certificate as trusted and creates the public key for the certificate to be used in SSL encryption.

A certificate from a Certificate Authority or a server functioning as a Certificate Authority for example Windows 2000 running Certificate Services can be uploaded to the device.

Note

A separate request is required for each Xerox device.

With SSL enabled (from the Connectivity / Protocols / HTTP selections of the Properties tab of Internet Services), and a digital certificate installed, remote users accessing the system over an HTTP based interface are assured of having their network communications protected against eavesdropping and tampering, using strong encryption. The only action required by the workstation user is to type https://, followed by the IP address (or fully qualified domain name) of the system, into the Address or URL box of the web browser. The subsequent acceptance of a Digital Certificate completes the exchange of the Public Key enabling the encryption process to proceed.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- An IP Address or Host Name must be configured on the device.
- DNS must be enabled and configured on the device.
- HTTP must be enabled so that Internet Services can be accessed.
- Ensure the system time configured on the device is accurate. This is used to set the start time for self signed certificates.

Creating a Digital Certificate

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Select **[Machine Digital Certificate Management]** in the directory tree.

   Note

   SSL cannot be implemented until a digital certificate is installed on the system.

7. Click on the **[Create New Certificate]** button.
8. Select either **Self Signed Certificate** or **Certificate Signing Request** radio button.

   Note

   A self-signed certificate is inherently less secure than installing a certificate signed by a trusted, third party Certificate Authority (CA). However, specifying a self-signed certificate is the easiest way to start using SSL. A self-signed certificate is also the only option if your company does not have a Server functioning as a Certificate Authority (Windows 2000 running Certificate Services, for example), or does not wish to use a third party CA.

9. Click on the **[Continue]** button.
10. If you selected **Self Signed Certificate**, fill out the form with your 2 Letter Country Code, State/Province Name, Locality Name, Organization Name, Organization Unit, Common Name, E-mail Address, and Days of Validity.
11. Click on the **[Apply]** button to continue. Values from the form will be used to establish a self-signed certificate, and you will be returned to the main page.

12. If you selected **Certificate Signing Request**, fill out the form with your 2 Letter Country Code, State/ Province Name, Locality Name, Organization Name, Organization Unit, and E-mail Address.
13. Click on the **[Apply]** button to continue. Values from the form will be used to generate a Certificate Signing Request.
14. When the process is complete, you will be prompted to save the Certificate Signing Request. Right click on the link and select **[Save Target As]**.
15. Save the Certificate to your hard drive and send it to a **Trusted Certificate Authority**.
16. When a signed certificate is received back from the Trusted Certificate Authority, upload the certificate to the device. To do this return to the **[Machine Digital Certificate Management]** screen, in the **Machine Digital Certificate** area, click on the **[Upload Signed Certificate]** button.
17. Click on the **[Browse]** button to locate the signed certificate from the Trusted Certificate Authority and click on the **[Open]** button.
18. Click on the **[Upload Certificate]** button.
19. If successful, the Current Status in the **Machine Digital Certificate** area will show **'A Self Signed Certificate is established on this device'**.

    Note

    For the upload to be successful, the signed certificate must match the CSR created by the device and must be in a format that the device supports.

20. To view installed certificates click the **[Trusted Certificate Authorities]** in the directory tree for **[Security]**. The installed certificate will appear in the list.

Enable Secure HTTP (SSL)

Once the device has a device server certificate, you can enable secure HTTP.

1. In the **Properties** menu, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[HTTP]**.
4. In the **Configuration** area, under **Secure HTTP (SSL),** select **[Enabled]**.
5. Enter the **[Secure HTTP Port Number]** if required.
6. Click on the **[Apply]** button.
7. Close your web browser and then access Internet Services screen again. The Security warning will display. Self-signed certificates usually cause browsers to display messages which question the trust of the certificate. Click the **[OK]** button to continue.

IP Sec

IP Sec (IP Security) comprises of the IP Authentication Header and IP Encapsulating Security Payload protocols, that secure IP communications at the network layer of the protocol stack, using both authentication and data encryption techniques. The ability to send IP Sec encrypted data to the printer is provided by the use of a public cryptographic key, following a network negotiating session between the initiator (client workstation) and the responder (printer or server). To send encrypted data to the printer, the workstation and the printer have to establish a Security Association with each other by verifying a matching password (shared secret) to each other. If this authentication is successful, a session public key will be used to send IP Sec encrypted data over the TCP/IP network to the printer. Providing additional security in the negotiating process, SSL (Secure Sockets Layer protocols) are used to assure the identities of the communicating parties with digital signatures (individualized checksums verifying data integrity), precluding password guessing by network sniffers.

IP Sec security settings are the means by which an administrator can configure multiple groups of hosts and groups of protocols. Also this feature is used to setup IPsec and IKE protocols on the printer.

The IP Sec implementation is a 'full' implementation, that the device can initiate a connection for print, scan and administration, and fully work with other industry IPsec nodes. IPsec is necessary to secure many protocols including:

- LPR and Port9100 printing
- FTP Filing
- Scan to EMail
- LDAP
- Internet Fax

Security Policies: To enable IP Sec

Note

IP Sec cannot be enabled until SSL (Secure Sockets Layer) is enabled on the device. To enable SSL on a device, the device needs to have a Server Certificate. For instructions to set up a Server Certificate, see Machine Digital Certificate Management on page 8-9.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Select **[IP Sec]** in the directory tree.
7. Ensure **[Security Policies]** tab is highlighted under the **IPsec** heading.
8. In the **Settings** area, place a check in the **[Enabled]** box to enable the IP Sec.
9. Click on the **[Apply]** button.

Define Policy

An IPsec Policy is a set of conditions, configuration options and security settings which enable two systems to agree on how to secure traffic between them. Multiple policies can be simultaneously active, however the scope and policy list order may alter the overall policy behavior.

10. In the **Define Policy** area, there are three policy options:
    - **Hosts**
    - **Protocols**
    - **Action**

    This area allows you to select setting for allowing or discarding Hosts and Protocol and what action to be taken.
11. For each individual option select settings from each drop-down menu.
12. Click on the **[Add Policy]** button.

Saved Policies

13. In the **Saved Policies** area, there will be a list of all the policies saved.
14. To delete a policy, highlight the policy and click the **[Delete]** button.
15. Also you can make individual policy to be prioritized by clicking the **[Promote]** and **[Demote]** buttons.

Disable IP Sec at the device

1. At the device, press the **<Log In/Out>** button to access the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, touch **[Enter]**.
3. If necessary, press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. In Tools menu, touch **[Security Settings]**.
5. Touch **[Image Overwrite Security]**.
6. Touch **[IP Sec]**.
7. Touch the **[Disable IP Sec]** button, then touch **[Close]**.
8. Press the **<Log In/Out>** button to exit Tools pathway.
9. Touch **[Logout]**.

Host Groups

This option displays all the Host Group saved and the details of each Host Group.

1. Click on the **[Host Groups]** tab under **IPsec** heading.
2. Host Groups can be deleted by highlighting a Host Group and clicking on the **[Delete]** button, if the Host Group selected is not being used by a security policy, then click on the **[OK]** button.
3. To add or edit a Host Group in the **IP Host Group** area click on the **[Add New Host Group]** button to add a new Host Group or highlight a Host Group and click on the **[Edit]** button to edit details of a Host Group.
   If you change a name of the Host Group that is being used in the **Security policy**, then the updated host group name will also reflect in the security policy details.
4. To define or modify a Host Group enter details in the **[Name]**, **[Description]** fields.
5. In the **Address List** area select atleast one set of network information.
   - Select either **[IPv4]** or **[IPv6]**.
   - For **Address Type** select either **[Specific]**, **[Subnet]** or **[All]** from the drop-down menu.
   - For **IP Address**, enter the IP Address.

6. Click on the **[Save]** button.

Protocol Groups

This option displays all the Protocol Group saved and the details of each Protocol Group.

1. Click on the **[Protocol Groups]** tab under **IPsec** heading.
2. Protocol Groups can be deleted by highlighting a Protocol Group and clicking on the **[Delete]** button, if the Protocol Group selected is not being used by a security policy, then click on the **[OK]** button.
3. To add or edit a Protocol Group in the **IP Protocol Group** area click on the **[Add New Protocol Group]** button to add a new Protocol Group or highlight a Protocol Group and click on the **[Edit]** button to edit details of a Protocol Group.
   If you change the name of a Protocol Group that is being used in Security policy, then the updated protocol group name shall also change in the security policy entry.
4. By clicking the **[Add New Protocol Group]** button, a new page will display allowing you to add the new protocol group.
5. In the **IP Protocol Group Details** area, enter details in the **[Group Name]** field.
6. Enter details in the **[Description]** area.
7. Check the required **Service Name** box.
8. In the **Custom Protocol** area, check the **Custom Protocol** box to select custom protocol, enter details in the **[Service Name]** field.
9. From the **[Protocol]** drop-down menu select the protocol.
10. Enter the port number in the **[Port]** field.
11. Select either **[Server]** or **[Client]** from the **[Device is]** drop-down menu.

    Note

    The Service Name, Protocol Type, Port Number and Device is fields for a Custom Protocol will be disabled when its associated checkbox is unchecked.

12. Click on the **[Save]** button.

Actions

This option displays the list of actions associated with the IPsec security policies.

1. Click on the **[Actions]** tab under **IPsec** heading.
2. Actions can be deleted by highlighting a Action and clicking on the **[Delete]** button, if the Action selected is not being used by a security policy, then click on the **[OK]** button.
3. To add or edit a Action in the **IP Protocol Group** area click on the **[Add New Action]** button to add a new Action or highlight a Action and click on the **[Edit]** button to edit details of a Action.
   If you change the name of a Action that is being used in Security policy, then the updated action name shall also change in the security policy entry.
4. By clicking the **[Add New Action]** button, a new page will display allowing you to add the new action.
5. In the **IP Action Details** area, enter details in the **[Action Name]** field.
6. Enter details in the **[Description]** area.
7. In the **Keying Method** area, select either **[Manual Keying]** or **[Internet Key Exchange (IKE)]**.
8. If you select Internet Key Exchange (IKE), enter details in the **[Pre-shared Key Passphrase]**.

    Note

    Only one Action may be created when selecting Internet Key Exchange (IKE) Keying Method.

9. Click on the **[Next]** button to display the **Step 2 of 2** screen.

If you Selected Manual Keying as the Keying Method:

1. In the **Mode Selections** area, select the **[IPsec Mode]** from the drop down menu, the default Mode is Transport Mode.
2. In the **Security Selections** area, select preferred option and enter the required informations.
3. Click on the **[Save]** button.

If you Selected Internet Key Exchange (IKE) as the Keying Method:

1. In the **IKE Phase 1** area, for **[Key Lifetime]** enter Key Lifetime details, and select required option from the **[DH Group]** drop-down menu and check the required **[Hash - Encrypt]** boxes.
2. In the **IKE Phase 2** area, select mode from the **[IPSec Mode]** drop-down menu.
   a. If you select **[Tunnel Mode]**, then select either **[Disabled]**, **[IPv4 Address]** or **[IPv6 Address]**.
   b. If you select **IPv4 Address** or **IPv6 Address**, enter IP Address details.
3. Select type of security from the **[IPsec Security]** drop-down menu.
4. Enter details in the **[Key Lifetime]** field.
5. Select the preferred option from the **[Perfect Forward Secrecy]** drop-down menu, default is '**None**' and check the boxes for **[Hash]** and **[Encryption]**.

   Note

   Encryption will not display if **[IPsec Security]** is set to **AH**.

6. Click on the **[Save]** button.

Trusted Certificate Authorities

The Trusted Certificate Authorities screen allows you to upload signed digital certificates via the device's web server. The certificate contains the public key and digital signature of a Trusted Certificate Authority, to support encryption via HTTPS/SSL.

Digital certificates and the enablement of SSL provides encryption for all workflows where the device is used as a HTTPS server.

Workflows include:

- Administration of the device via Internet Services
- Printing via Internet Services
- Printing via IPP
- Scan Template Management
- Workflow Scanning via HTTPS
- Administration of Network Accounting

The device exports the signed certificate to the client to establish an SSL/HTTPS connection.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Select **[Trusted Certificate Authorities]** in the directory tree.

Request a Machine Root Certificate

The device has the ability to sign its own Certificate Signing Request (CSR) by using a Device Generic Certificate Authority.

1. Right-click on the **[Download the Generic Xerox Device CA]** link which appears at the bottom of the screen, under the **Installed Certificates** box.
2. Select **[Save Target As.]**.
3. Browse to the location where you want to save the **cacert.pem** file and click on **[Save]**.
4. The **cacert.pem** file is now ready to be uploaded to any device needing a Machine Root Certificate.

Install a Root Certificate

To complete this procedure you must have a digital certificate available. For instructions to configure a digital certificate, refer to Machine Digital Certificate Management on page 8-9.

1. At the **Trusted Certificate Authorities** screen, click on the **[Add]** button.
2. Click on the **[Browse]** button to locate the signed certificate from the Trusted Certificate Authority, click on the **[Open]** button.
3. Click on the **[Upload Certificate Authority]** button.
4. The digital certificate will appear in the list of **Installed Certificates**.

Immediate Image Overwrite

Overview

The Immediate Image Overwrite feature provides security conscious customers with the ability to overwrite the device's hard disk to protect classified or private information.

The device's hard disk stores data similarly to the way a hard drive functions on a personal computer, but with the data encrypted for extra protection. When Print, Copy, E-mail, Internet Fax and Scan jobs are submitted to the device, information is stored on the device's hard disk (if these features are installed and configured on the device). Immediate Image Overwrite automatically erases image data on a job by job basis, once completed at the device.

Immediate Image Overwrite and Internet Fax Jobs

Note

Internet Fax jobs are not overwritten until the job's Delivery Status Notifications (DSN's) and Message Disposition Notifications (MDN's) have been received, or timeout occurs, i.e. the job is not overwritten until after the **Delivery Confirmed** state or **Sent state** is exited. This means that the job may not be overwritten for up to 72 hours as this is the maximum timeout setting for an Internet Fax job.

Information Checklist

Before starting the installation procedure, please ensure the following items is available or has been performed:

- Ensure the device is fully functioning in its existing configuration prior to installation.

Verify that Immediate Image Overwrite is an Installed Option

Print a Configuration Report as follows:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**

Immediate Image Overwrite Status

When Immediate Image Overwrite is configured on the device any job that is overwritten will have its overwrite status displayed in the Completed Jobs queue details window.

To view Overwrite Status at the Device

1. Press the **<Job Status>** button.
2. Touch the **[Other Queues]** button (if necessary).
3. Touch the **[All Completed Jobs]** button.
4. Touch a job in the queue.
5. View the Immediate Overwrite Status. This will appear as Successful or Failed.
6. Touch **[Close]**.

Disabling or Enabling Immediate Image Overwrite

Overwrite Security can be disabled or enabled at any time, as follows.

At the Device

1. Press the **<Log In/Out>** button to access the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. If necessary, press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. From Tools, touch **[Security Settings]**.
5. Touch **[Image Overwrite Security]**, then **[Immediate Overwrite]**.
6. Touch **[Enable]** or **[Disable]**, then touch **[Save]**. The change in status will be immediately effective.
7. Press the **<Log In/Out>** button, touch **[Logout]** to log out of the Tools pathway.

On Demand Overwrite

Overview

The On Demand Overwrite feature provides security conscious customers with the ability to overwrite the device's hard disk to protect classified or private information.

The device's hard disk stores data similar to the way a hard drive functions on a personal computer, but with the data encrypted for extra protection. When Print, Copy, E-mail, Internet Fax and Scan jobs are submitted to the device, information is stored on the device's hard disk (if these features are installed and configured on the device).

The On Demand Overwrite feature can be used by a System Administrator to overwrite the image data. The process takes approximately 20 minutes to complete. The device is taken offline until the overwrite is complete and any existing jobs in the print queue are terminated.

Information Checklist

Before starting the procedure, please ensure the following item is available or has been performed:

- Ensure the device is fully functioning in its existing configuration prior to installation.

Verify that On Demand Image Overwrite is an Installed Option

If a Configuration Report did not print during SIM installation, print the report as follows:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**

Perform an Image Overwrite at the Device

This procedure will overwrite the image data from the hard disk. This excludes Embedded Fax data, when this feature is installed on the device.

Note

All existing jobs (excluding Embedded Fax), regardless of their state, shall be deleted and all job submission will be prohibited for the duration of the overwrite. The power on/off button will be ignored during image overwrite.

The device should not be in diagnostics mode when the Overwrite is started. (The device screen indicates a status of 'Diagnostics Mode'- this mode is used by a Customer Service Representative when servicing the device.) The device should not be used to perform any jobs and the power should not be switched off while an Overwrite is being performed.

At the Device

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. If necessary, press the **<Machine Status>** button, then touch the **[Tools]** tab.

4. From Tools, touch **[Security Settings]**.
5. Touch **[On Demand Overwrite]**.
6. Select either:
   - **[Standard]** - will exclude Print File directories and Scan to Mailbox jobs, Fax Dial directories and Mailbox contents
   - **[Full]** - everything from memory and hard disk(s) will be overwritten.
7. Touch **[Overwrite Now]** to start the Image Overwrite process.
8. The Overwrite confirmation screen will appear. The device will be taken offline and will be unable to receive any incoming jobs. The Image Overwrite will proceed to overwrite all image data on the hard disk. The process will take approximately 20 minutes for Standard overwrite and Approximately 60minutes for a Full overwrite.

   Note

   To cancel the overwrite procedure touch the **<Abort>** button. Enter the current administrator password (the default is **[1111]**) and touch **[Enter]**. The overwrite procedure may have already started at this stage but will return to normal operation. Select the **[Back]** button if you want to continue with the overwrite.

9. Following completion of the Overwrite the On Demand Overwrite completion screen appears. Touch **[Close]**. The network controller will reboot and network functionality will be unavailable for several minutes.
10. Once rebooted, the Disk Overwrite confirmation report will print. This details the status and time of the overwrite.

    To verify the overwrite has completed view the Confirmation Sheet, under Confirmation Details. The Job Information: Status ESS Disk should read '**SUCCESS**'.

You have completed the steps.

Perform an Image Overwrite over the Network

When the device has a network controller and is connected over the network, it is possible to run the Image Overwrite function using a web browser. This is performed using Internet Services.

Note

All existing jobs, regardless of their state, shall be deleted and all job submission will be prohibited for the duration of the overwrite. The power on/off button will be ignored during image overwrite.

The device should not be in diagnostics mode when the Overwrite is started. (The device screen indicates a status of 'Diagnostics Mode'- this mode is used by a Customer Service Representative when servicing the device.) The device should not be used to perform any jobs and the power should not be switched off while an Overwrite is being performed.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the device is fully functioning on the network.
- Ensure TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 2-5, so that the web user interface (Internet Services) can be accessed.
- Ensure that no one is currently using the device.

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[On Demand Overwrite]** link.
7. Click **[Manual]** in the directory tree.
8. Click on the **[Start]** button for either **Standard** or **Full**. image overwrite.
   - **Standard Image Overwrite** will delete all image data from memory and hard disk, except:
     - Jobs and folders stored in the Reprint Saved Jobs feature.
     - Jobs stored in the Scan to Mailbox feature (if installed).
     - Fax Dial Directories (If fax card is installed).
     - Fax Mailbox contents (If fax card is installed).

   This will take approximately 20 minutes. The overwrite process cannot be cancelled and the device will remain offline until it is completed.

   - **Full Image Overwrite** will delete all image data from memory and hard disk(s). Data to be Deleted INCLUDES:
     - Jobs and folders stored in the Reprint Saved Jobs feature.
     - Jobs stored in the Scan to Mailbox feature (if installed).
     - Fax Dial Directories (If fax card is installed).
     - Fax Mailbox contents (If fax card is installed).

   This will take approximately 60 minutes. The overwrite process cannot be cancelled and the device will remain offline until it is completed.
9. Click on the **[OK]** button. The overwrite will commence. The device will be taken offline and will be unable to receive any incoming jobs. Any existing jobs in the queue will be deleted.
10. Following completion of the Overwrite, the On Demand Overwrite completion screen appears. Touch **[Close]**. The network controller will reboot and network functionality will be unavailable for several minutes. Once rebooted, the Disk Overwrite confirmation report will print. This details the status and time of the overwrite.

    To verify the overwrite has completed view the Confirmation Sheet, under Confirmation Details. The Job Information: Status ESS Disk should read '**SUCCESS**'.

Schedule a Daily Overwrite

A TCP/IP network-connected device can be set to overwrite image data on a daily basis. To schedule a daily overwrite, perform the following steps.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address or Location field. Press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[On Demand Overwrite]** link.
7. Select **[Scheduled]** in the directory tree.
8. Select the required frequency from the **[Frequency]** drop down list to enable the Overwrite.

9. Specify the time for the Overwrite in **[Hours]**, **[Minutes]** (24-Hour Clock). The device will be taken offline each day at the time specified to perform the overwrite.
   If **[Weekly]** is selected, you can select a day in the week for the schedule event to run on that day of the week at the time you specify.
   If **[Monthly]** is selected, you can select a day between 1 and 28 for the task to run on that date of the month.

PostScript (R) Passwords

The PostScript language has some powerful utilities that could be used to compromise the security of a system. These utilities can be password protected so as to prevent abuse. This feature is concerned with the ability to set the various passwords. In addition, we have extended the PostScript language with custom operators; the same passwords could be used to secure the custom extensions.

Without a password in place, anyone with slight knowledge of Postscript can potentially abuse the system. They can use the **Startjob** and **Exitserver** operators, change the system parameters, and run jobs that can re-define PostScript operators etc.

There are three passwords defined in the PostScript Password page, as follows:

- **Start Job Password** - A write-only string. Authorizes the use of startjob and exitserver
- **Run Start Job** - An integer. Controls the execution of the Sys/Start file, which runs as an unencapsulated job and loads definitions into VM. This parameter should only ever be set to 0 or 1 in normal use.
- **System Parameters Password -** A write only string. Controls use of the setsystemparams and setdevparams operators

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click **[PostScript (R) Passwords]** in the directory tree.
7. On the **PostScript (R) Passwords** page, in the **Run Start Job** area select either **[Disabled]** or **[Enabled]** for **StartupMode**.
8. Enter details in the **[Password]** and **[Retype Password]** box for **System Parameters Password** and/or **Start Job Password**.
9. You can also check the **Select to save new password** box for **System Parameters Password** and/or **Start Job Password**.
10. When finished, click on the **[Apply]** button.

9 Extensible Services Setup

Xerox Extensible Interface Platform (EIP) is a software platform inside many Xerox MFPs that allows independent software vendors and developers personalized and customized document management solutions that you can access directly from the MFP touch screen. These solutions can leverage your existing infrastructure and databases.

For example, a hospital could customize the device to help manage patient forms. By touching an icon on the display, a healthcare worker could access the hospital's web based document management system and browse a list of patient forms.

Users can quickly scan and capture paper documents, preview thumbnails, and add them to frequently used document storage locations. For example:

A tutor can scan notes directly to a specific course repository for students to access

A student can scan assessment papers to their course folder for their tutor to mark.

Xerox Extensible Interface Platform utilizes web based Xerox Partner solutions including:

- **Xerox Secure Access Unified ID System**: Secure Access integrates with your personalized ID badge. This convenient security solution allows people to simply swipe their ID badge at the device to unlock access to features that can be tracked for accounting and regulatory requirements. Secure Access is also the key to the personalized experience at the device.
- **Xerox Scan to PC**: This solution bridges the gap between documents, PDFs and paper, helping you to personalize your Xerox workflow scanning and PDF workflow. It also gives you the ability to customize, directly from your desktop, the scanning menus available to you on your Xerox EIP enabled device. This makes it easy to securely scan from the device to specific folders on your workstation.

Other software such **Omtool™**, **Equitrac™** and **FreeFlow™ SMARTsend™** are available, which enables users to access document repositories at the device display screen.

Additional resources may be required on the device depending on the solution.

For further information, contact your Xerox Sales Representative.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure the device is fully functioning on the network.
- Ensure your XEIP solution is installed and functioning. To enable EIP applications, an **InstallCustomServices.dlm** has to be installed on the device.
- Ensure SSL is enabled on the device. For further information refer to the Digital Certificate Management topic in this System Administrator's Guide.

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Select **[Manual Upgrade]** in the directory tree.
8. In the **[Manual Upgrade]** area, click on the **[Browse]** button to browse to where the **InstallCustomServices.dlm** is located.
9. Select the file, click on the **[Open]** button, then click on the **[Install Software]** button.
10. If you have not already done so, create a digital certificate on your device, by referring to Machine Digital Certificate Management on page 8-9. Set the days of validity to 9999.
11. Ensure that Secure HTTP (SSL) is enabled on your device. Click **[Properties]**, **[Connectivity]**, **[Protocols]**, and finally **[HTTP]**.
12. Click on the **[Enable]** radio button to enable **Secure HTTP (SSL)**.
13. Click on the **[Apply]** button. Note that the screen will disappear temporarily, and you will need to refresh your browser
14. To enable Extensible Service Registration, from the HTTP web page, select **[Web Services]** from the selection box near the top of the page. Note that the two available selections are **HTTP** and **Web Services**.
15. Check the **[Extensible Service Registration]** checkbox. Note that if the Extensible Service Registration web service is not present in the list, this indicates that the software install was not completed or failed.
16. Click on the **[Apply]** button.

At the Device

1. Press the **[Services]** button.
2. Touch the EIP Application button that you registered. Your XEIP workflow is accessible from the new button.

10 Workflow Scanning

Workflow Scanning allows a user to scan an original document, convert it to an electronic file, and distribute and archive that file in a variety of ways. The final destination of the electronic file depends on the template chosen by the user at the device's user interface. The template may reside on the device, or may be cached on the device from a pool of templates pulled from a remote server. The scanned file will be stored on a pre-determined network server and then, with the help of server or desktop software:

- routed to a user's PC desktop for viewing or editing.
- integrated with a variety of popular document management and workflow applications.
- sent to a network directory or filing location for later retrieval.
- sent to an e-mail distribution list.

FreeFlow SMARTsend has replaced CentreWare Workflow Scanning Services

Note

FreeFlow SMARTsend combines and enhances the powerful features of two Xerox products - FlowPort and CentreWare Workflow Scanning Services - to deliver one integrated software application.

FreeFlow SMARTsend scanning services

Built on the Microsoft .NET platform, this server-based software works with new and legacy Multifunction Systems to enable hardcopy documents to be scanned in black and white or color, and converted into such standard digital formats as PDF, JPEG, and TIFF. This web based application requires no additional client software installation and uses wizards to simplify workflow (template) creation. Once a workflow, or distribution process, is created, it can be saved as a paper or electronic cover sheet. The cover sheet can be set up to direct the scanned file to a wide variety of destinations. Such destinations include an e-mail address or distribution list, network folder, FTP folder, remote printer, web URL, Domino.doc, Domino, Microsoft SharePoint and Xerox DocuShare.

Scan to PC Desktop

For information regarding the additional use of Scan to PC Desktop, including Scansoft Paperport and Textbridge Pro applications, consult your Xerox Sales Representative.

Workflow Scanning User Authentication

Authentication can be enabled to prevent unauthorized access to the Workflow Scanning feature. If Authentication is enabled, users will be prompted to enter a network user name and password, or a PIN, before they can access the Workflow Scanning feature. For a full description of the Authentication feature refer to the Authentication section of this guide. Authentication can be configured after Workflow Scanning has been installed.

Device Authentication

If using a SMARTsend server, a valid Windows account must be created on the SMARTsend Server for the device's authentication. The account enables each device to communicate with the SMARTsend server to exchange template information and other configuration data. For account creation instructions, refer to the FreeFlow SMARTsend Installation and Administration Guide.

Template Considerations when using SMARTsend

A single Xerox device cannot use both CentreWare Workflow Scanning services and SMARTsend. If legacy CentreWare Workflow Scanning Services templates need to be utilized within SMARTsend, use the SMARTsend Template Importer to import the desired templates, as stated in the FreeFlow SMARTsend Installation and Administration Guide.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the device is fully functioning on the network.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.

  This is required to access Internet Services to configure Workflow Scanning. The Internet Services function is accessed through the embedded HTTP server on the device and allows System Administrators to configure scan settings by using an Internet browser.

Configure a Scan Filing Location

Scanning with the device is accomplished through user selection of templates on the device that route scanned jobs to network servers. After storage on the server, the files can be retrieved at any properly configured networked workstation. A dedicated file server is not required to receive scans. A dedicated server is required, however, for the installation and use of SMARTsend software to remotely manage the pool of templates (workflows), displayed locally to device users, if so desired. Scanning is configured on the device using one of the file transfer options below.

- **FTP (File Transfer Protocol):** Requires an FTP server running on a server or a workstation.
- **NetWare NCP (NetWare Core Protocol):** Available for filing to a NetWare server.
- **SMB (Server Message Block):** Available for filing to an environment that supports the SMB protocol.
- **HTTP/HTTPS:** Supports scans to a web server using a CGI script.

File Transfer Protocol (FTP)

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure that File Transfer Protocol (FTP) services are running on the Server or Workstation where images scanned by the device will be stored.

Write down the IP Address or Host Name.

- Create a folder within the FTP root. This is the Scan Repository.

  Write down the Directory Path Structure.
- Create a user account and password which has read and write access to the folder within the FTP root.

  Write down the user Account and Password details.
- Test the FTP connection by logging into the Scan Repository directory from a PC with the user account and password:
  - Create a new folder within the directory
  - Delete the folder.

Enter the Scan Repository Details via Internet Services

1. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[File Repository Setup]** in the directory tree.
8. Click on the **[Add New]** button in the File Repository Setup area, or the **[Edit]** button (If the default File Repository has been set).

   Note

   During device configuration, SMARTsend (if used) overwrites the Default Repository and Template Pool scan settings. If certain applications will use Default Repository settings, not matching SMARTsend settings, reconfigure the applications to use an Alternate Repository before configuring the device with SMARTsend's Add/Update feature.
9. Enter a name to describe the filing destination template in the **[Friendly Name]** entry box.
10. Select FTP from the **[Protocol]** drop down menu.
11. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
12. Enter the **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the FTP location.
13. Type in the path to the location of the scan folder in **[Document Path]**. Enter the full path to the directory, starting at the root of FTP services. For example: */directory name/directory name*.
14. Select a radio button for **[Login Credentials to Access the Destination]**. Select **[Authenticated User]** to have your Authentication Server determine user access to the file server. Select **[Prompt at User Interface]** to have the file server determine user access. Select **[System]** to have the system directly log in to the file server.
15. Enter a **[Login Name]** and **[Password]**, if the system will be directly accessing the file server.
16. Click on the **[Save]** button to accept the changes.
17. To configure General Settings, select **[General]** in the directory tree under Workflow Scanning.
18. To print a Confirmation Sheet after every scan job, select **[On]** from the drop down menu. The Confirmation Sheet specifies the status of the job, and the file location if the scan was successful.
19. New distribution templates created for the device can be set to automatically update by entering a time in the **[Refresh Start Time]** area under **Distribution Templates**. Note that Distribution Templates can

be created with specific scan settings and destinations. For further information refer to Configuring the Default Template on page 10-11

20. **Login Source** settings control user access to a pool of templates stored on a remote server. Communications to the server, including entry of the required device Login Name and Password, are set up by clicking on the **[Advanced]** link, then selecting **[Template Pool Setup]** in the directory tree, in the Internet Services directory tree. Select **[Authenticated User]** to have the Authentication Server control remote template pool access. Select **[Prompt at User Interface]** to have a standalone server prompt device users for access. This works well for small offices, without an Authentication server. Select **[Prompt if Authenticated User Does Not Match Template Owner]** to prompt authenticated users accessing templates containing either no or other users' owner names.
21. Check the **[User Name]** and **[Domain]** boxes if you want these to appear on the Job Log. The Job Log works with the Document Management Fields feature and is filed with the scan job.
22. Click **[Apply]**.

Go to the Device

23. Touch the **[Workflow Scanning]** icon on the touch screen.
24. Touch **[All Templates]**.
25. Select **[All Templates]** from the **[All Templates]** drop down menu.
26. Select **[Advance Setting]** tab.
27. Touch the **[Update Template]** icon.
28. Touch **[Update Now]**.
29. Touch **[Confirm]**, touch **[Use Partial List]**.
30. Touch **[Close]**.
31. Touch the **[Workflow Scanning]** tab.
32. Select the **[Default]** template and place a document in the document handler.
33. View template details on the monitor.
34. Press the **[Start]** button to scan the document.
35. Check the scan folder on your file server to verify the image was filed.

The Next Step is to proceed to the General Settings, see Optional Step: Configure General Settings on page 10-10.

NetWare NCP (NetWare Core Protocol)

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure the device is fully functioning on the network prior to installation.
- Ensure the NetWare protocol is enabled on your device.

  How to check that the NetWare protocol is enabled on your device

  Print a Configuration Report to verify that NetWare protocol is enabled on your device.

  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Information Pages]**.
  d. Touch **[Configuration Report]**.

e. Touch **[Print]**, then touch **[Close].**

The Configuration Report will print. Verify the NetWare settings configured under Network Setup.

NetWare should read Enabled.

For instructions on how to enable NetWare refer to the NetWare topic in the Protocol section of this guide.

- **Designate or create a new directory on the NetWare server** to be used as the scan filing location (repository). Note the server name, server volume, directory path, the NDS Context and Tree, if applicable.
- **Create a user account and password with access to the scan directory**. When a document is scanned the device logs in using the account, transfers the file to the server and then logs out. Note the user account and password.
- **Test your settings** by logging in to the scan directory from a PC with the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function check the user account access rights.

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[File Repository Setup]** in the directory tree.
8. Click on the **[Add New]** button in the File Repository Setup area, or the **[Edit]** button (If the default File Repository has been set).

   Note

   During device configuration, SMARTsend (if used) overwrites the Default Repository and Template Pool scan settings. If certain applications will use Default Repository settings, not matching SMARTsend settings, reconfigure the applications to use an Alternate Repository before configuring the device with SMARTsend's Add/Update feature.

9. Enter a name for the filing destination template in the **[Friendly Name]** box.
10. Select **[NetWare]** from the **[Protocol]** drop down menu.
11. Enter the server name where the scan filing repository is located, in the **[Server Name]** box.
12. Enter the server volume in the **[Server Volume]** box.
13. Enter the context and tress in the **[NDS Context]** and **[NDS Tree]** boxes (NetWare 4.x, 5.x, 6.x IPX only.) for the repository. For NDS enter a name context. For bindery and bindery emulation, leave these fields blank.
14. Enter the path to the scan filing location in the **[Document Path]** box.
15. Select a radio button for **[Login Credentials to Access the Destination]**. Select **[Authenticated User]** to have your Authentication Server determine user access to the file server. Select **[Prompt at User**

Interface] to have the file server determine user access. Select **[System]** to have the system directly log in to the file server.

16. Supply a **[Login Name]** and **[Password]** if the system will be directly accessing the file server.
17. Click on the **[Save]** button to accept the changes.
18. To configure General Settings, select **[General]** in the directory tree.
19. To print a Confirmation Sheet after every scan job select **[On]** from the drop down menu.
20. New distribution templates created for the device can be set to automatically update by entering a time in the **[Refresh Start Time]** area.
21. Login Source settings control user access to a pool of templates stored on a remote server. Communications to the server, including entry of the required device Login Name and Password, are set up by selecting **[Advanced]**, then **[Template Pool Setup]**, in the Internet Services directory tree. Select **[Authenticated User]** to have the Authentication Server control remote template pool access. Select **[Prompt at User Interface]** to have a stand alone server prompt device users for access. This works well for small offices, without an Authentication server. Select **[Prompt if Authenticated User Does Not Match Template Owner]** to prompt authenticated users accessing templates containing either no or other users' owner names.
22. Check the **[User Name]** and **[Domain]** boxes if you want these to appear on the Job Log. The Job Log works with the Document Management Fields feature and is filed with the scan job.
23. Click on the **[Save]** button to accept changes made.

At the Device

1. Touch the **[All Services]** button.
2. Touch **[Workflow Scanning]** on the touch screen.
3. Touch the **[Workflow Scanning]** tab.
4. Select **[All Templates]** from the **[All Templates]** drop down menu.
5. Select the **[Default Template]** and place a document in the document handler.
6. View template details on the monitor.
7. Press the **[Start]** button to scan the document.
8. Check the scan repository on your server to verify the image was filed.

The Next Step is to proceed to the General Settings, see Optional Step: Configure General Settings on page 10-10.

Server Message Block (SMB)

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Create a shared folder to be used as a scan filing location (repository) for scanned documents. Note the Share Name of the folder and the Computer Name or Server Name.
- Create a user account and password for the device with full access rights to the scan directory. Note the user account and password.
- Test the settings by attempting to connect to the shared folder from another PC by logging in with the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function check the user account access rights.

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[File Repository Setup]** in the directory tree.
8. Click on the **[Add New]** button in the File Repository Setup area, or the **[Edit]** button (If the default File Repository has been set).

   Note

   During device configuration, SMARTsend (if used) overwrites the Default Repository and Template Pool scan settings. If certain applications will use Default Repository settings, not matching SMARTsend settings, reconfigure the applications to use an Alternate Repository before configuring the device with SMARTsend's Add/Update feature.

9. Enter a name for the filing destination template in the **[Friendly Name]** box.
10. Select **SMB** from the **[Protocol]** drop down menu.
11. Select either the **[IPv4 Address]** or **[Host Name]** radio button.
12. Enter the **[IPv4 Address]** and **[Port]** or **[Host Name]** and **[Port]** of the computer where the scan filing repository (SMB server or workstation) is located.
13. Enter the Share Name in the **[Share]** box.
14. Enter the Document Path (as it relates to the share) where the scan filing repository is located, in the **[Document Path]** box. For example: If the path is *sharename\wc\scans, enter \wc\scans*.
15. Select a radio button for **[Login Credentials to Access the Destination]**. Select **[Authenticated User]** to have your Authentication Server determine user access to the file server. Select **[Prompt at User Interface]** to have the file server determine user access. Select **[System]** to have the system directly log in to the file server.
16. Supply a **[Login Name]** and **[Password]** if the system will be directly accessing the file server.
17. Click on the **[Save]** button to accept the changes.

Configure General Settings

18. Select **[General]** in the directory tree.
19. To print a Confirmation Sheet after every scan job select **[On]** from the drop down menu.
20. New distribution templates created for the device can be set to automatically update by entering a time in the **[Refresh Start Time]** area.
21. Login Source settings control user access to a pool of templates stored on a remote server. Communications to the server, including entry of the required device Login Name and Password, are set up by selecting **[Advanced]**, then **[Template Pool Setup]**, in the Internet Services directory tree. Select **[Authenticated User]** to have the Authentication Server control remote template pool access. Select **[Prompt at User Interface]** to have a standalone server prompt device users for access. This works well for small offices, without an Authentication server. Select **[Prompt if Authenticated User Does Not Match Template Owner]** to prompt authenticated users accessing templates containing either no or other users' owner names.
22. Check the **[User Name]** and **[Domain]** boxes if you want these to appear on the Job Log. The Job Log works with the Document Management Fields feature and is filed with the scan job.
23. Click on the **[Save]** button to accept changes made.

At the Device

24. Touch the **[Workflow Scanning]** button on the touch screen.
25. Touch the **[Workflow Scanning]** tab.
26. Touch the **[Show]** button.
27. Select **[All Templates]** from the **[All Templates]** drop down menu.
28. Select the **[Default]** template and place a document in the document handler.
29. View template details on the monitor.
30. Press the **[Start]** button to scan the document.
31. Check the scan folder on your file server to verify the image was filed.

The Next Step button is to proceed to the Configure the Default Template instructions.

HTTP/HTTPS

Before starting the Installation procedure, please ensure that the following items are available and/or the tasks have been performed:

- Ensure that HTTP/HTTPS services and a web service (such as Apache) are running on the server, where POST requests and scanned data will be sent for processing by a CGI script. Note the IP address or host name.

  Note

  HTTP and HTTPS protocol both require server-side scripts to allow files to be transferred to your HTTP server from your device.
  CGI (Common Gateway Interface) script. A program that is run on a web server, in response to input from a browser. The CGI script is the link between the server and a program running on the system, i.e a database.

- Download a sample script:
  a. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
  b. Click the **[Properties]** tab.
  c. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
  d. Click on the **[Services]** link.
  e. Click on the **[Workflow Scanning]** link.
  f. Select on the **[File Repository Setup]** link.
  g. Click on the **[Add New]** button in the File Repository Setup area, or the **[Edit]** button (If the default File Repository has been set).
  h. Select **[HTTP]** or **[HTTPS]** from the **[Protocol]** drop-down menu.
  i. Click on the **[Get Example Scripts]** link under *Script Path and Filename:* to download an example script in **PHP**, **ASP** or **Perl** language:
  j. Select an appropriate *Script Language* file which is supported by your HTTP Scan Repository server.
  k. Right click on the required script and select **[Save Target As...]** to save the file to your HTTP Scan Repository server.
  l. Save the **[.zip]** or **[.gz]** file to a location on the desktop and extract it.
  m. Extract the downloaded file to the root of the **[Web Services]** home directory.
  Write down the path and filename as you will need it later.
- Create a login account for the device on the web server.

a. Create a home directory for the device.
b. Add a bin directory to the home directory.
c. Place an executable CGI script in the bin directory.
d. Make a note of the complete path to the executable CGI script.
When a document is scanned, the device logs in using the account, sends a POST request along with the scanned file, then logs out. The CGI script handles the remaining details of file transfer.

- Create a directory on the web server, or an alternate server, to be used as a scan filing location (repository).
  a. Set appropriate read and write permissions.
  b. Make a note of this directory's path.
- Test the connection.
  a. Log in to the device's directory on the web server.
  b. Send a POST request and file to the web server.
  c. Check to see if the file was received at the repository.
- The script can be defined with script_name.extension or by path/script_name.extension.

At your Workstation:

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[File Repository Setup]** in the directory tree.
8. Select **[Add]** in the Default File Destination box, or **[Edit]** if the default File Destination has previously been configured.

   Note

   During device configuration, SMARTsend (if used) overwrites the Default Repository and Template Pool scan settings. If certain applications will use Default Repository settings, not matching SMARTsend settings, reconfigure the applications to use an Alternate Repository before configuring the device with SMARTsend's Add/Update feature.

9. Enter a name to describe the filing destination template in the **[Friendly Name]** box.
10. Select HTTP or HTTPS from the **[Protocol]** drop down menu.
11. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
12. Enter the **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the HTTP or HTTPS server. For HTTPS communications, click **[View Trusted SSL Certificates]** to verify that the device has a digital certificate installed. Optionally, you can check the **[Validate Repository SSL Certificate]** box.
13. Type in the path (starting at root) to the CGI script. Click **[Get Example Scripts]** for working scripts.
14. Type in the path to the location of the scan folder in **[Document Path]**. For web server directories, type in the path starting at root.
15. Select a radio button for **Login Credentials to Access the Destination**. Select **Authenticated User** to have your Authentication Server determine user access to the web server. Select **Prompt at User**

Interface to have the web server determine user access. Select **System** to have the system directly log in to the web server. Select None for rare instances where a login is not required.

16. Supply a **[Login Name]** and **[Password]**, if the system will be directly accessing the web server.
17. Click on the **[Save]** button to accept the changes.
18. To configure General Settings, select **[General]** in the directory tree.
19. To print a Confirmation Sheet after every scan job, select **[On]** from the drop down menu. The Confirmation Sheet specifies the status of the job, and the file location if the scan was successful.
20. New distribution templates created for the device can be set to automatically update by entering a time in the **[Refresh Start Time]** area under Distribution Templates. Note that Distribution Templates can be created with specific scan settings and destinations. Refer to Configure the Default Template later in this document, for further information.
21. Login Source settings control user access to a pool of templates stored on a remote server. Communications to the server, including entry of the required device Login Name and Password, are set up by selecting **[Advanced]**, then **[Template Pool Setup]**, in the Internet Services directory tree. Select **[Authenticated User]** to have the Authentication Server control remote template pool access. Select **[Prompt at User Interface]** to have a standalone server prompt device users for access. This works well for small offices without an Authentication server. Select **[Prompt if Authenticated User Does Not Match Template Owner]** to prompt authenticated users accessing templates containing either no or other users' owner names.
22. Check the **[User Name]** and **[Domain]** boxes if you want these to appear on the Job Log. The Job Log works with the Document Management Fields feature and is filed with the scan job.
23. Click on the **[Save]** button to accept changes made.

Go to the Device

24. Touch the **[Workflow Scanning]** button on the touch screen.
25. Touch the **[Workflow Scanning]** tab.
26. Select **[All Templates]** from the **[All Templates]** drop down menu.
27. Select the **[Default]** template and place a document in the document handler.
28. View template details on the monitor.
29. Press the **[Start]** button to scan the document.
30. Check the scan folder on your file server to verify the image was filed.

The Next Step button is to proceed to the Configure the Default Template instructions.

Optional Step: Configure General Settings

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Workflow Scanning]** link.
6. Click on the **[General]** link.

Confirmation Sheet

Note

The Confirmation Sheet specifies the success or failure of the Workflow Scanning job.

7. Select one of the following options from the **[Confirmation Sheet]** drop-down menu:
   a. **On** - Prints a Confirmation Sheet after every Workflow Scanning job
   b. **Errors only** - Prints a Confirmation Sheet only when the job is unsuccessful.
   c. **Off** - Turns off the Confirmation Sheet printing function.

Distribution Templates

8. Users can create Scan Templates with specific Workflow Scanning settings and destinations. If you want the device to automatically update templates stored in the Template Pool (a repository on the network), then enter the required time for the update in the **[Refresh Start Time]** area.
9. To update the Template Pool List manually, click on the **[Refresh Template List Now]** button.

Note

The Refresh Template List capability only applies to templates stored in a Template Pool. Templates stored on the device are updated automatically.

Template Distribution Repositories

10. **[Login Source]** control user access to a pool of templates stored on a remote server. Communications to the server, including entry of the required device Login Name and Password, are set up by selecting Advanced, then Template Pool Setup, in the Internet Services directory tree. Select **[Authenticated User]** to have the Authentication Server control remote template pool access. Select **[Prompt at User Interface]** to have a standalone server prompt device users for access. This works well for small offices without an Authentication server. Select **[Prompt if Authenticated User Does Not Match Template Owner]** to prompt authenticated users accessing templates containing either no or other users' owner names.

Job Log

11. Click on the **[Username]** and **[Domain]** / **[Tree]** / **[Realm]** boxes if you want these to appear in the Job Log when users log in to the device when Network Authentication is enabled.
12. Click on **[Apply]**.

Configuring the Default Template

The default template is created for the device, using Internet Services or SMARTsend software on the remote template pool server, and appears as DEFAULT in the list of templates on the device. The default template consists of configured scan settings and at least one network filing location. Once the default template has been configured, all subsequent templates, created with Internet Services or SMARTsend software, inherit the settings. Users can modify these settings with any new templates they create. The default template settings, however, can only be changed by the System Administrator. The default template also cannot be deleted from either the local or remote template pool.

1. At your Workstation, open the web browser and enter the *IP address* or location of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.

4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[Default Template]** in the directory tree.

Destination Services

8. If available, select the desired service by clicking on either the **[Fax]** or **[File]** links.

   Note

   The Fax service requires the Server Fax feature to be installed on the device.

Filing Options

9. Select **[Edit]**.
10. Enter a name in the **[Document Name]** box for the document scanned.
11. Select the Document Format from the following options:

    TIFF: Each scanned original is converted into one TIFF image file. All of these files will be stored in a directory (foldername.xsm).

    Multi-Page TIFF: A single TIFF file will be created containing all the pages of the document.

    JPEG: Creates standard JPEG File Interchange Format (.jpg) documents with one image per file.

    PDF: (Portable Document Format). The PDF image format is a multipage TIFF image enclosed within a PDF wrapper.
12. Click on the **[Apply]** button to accept the changes.

File

Once a scan filing destination has been configured from within the File Repository Setup section of Internet Services, it can be added to the Default Template.

To Add a New Filing Destination:

1. Click on the **[Add]** button next to the File Destinations section.
2. Select the required **[Filing Policy]** from the drop down menu.
3. Click on the **[Apply]** button to accept the changes.

Fax Destinations

Note

This option will only be available if the Server Fax option is installed on the device and Fax was selected as a Destination Service.

4. Select **[Destination Services]** and check the **[Fax]** box.
5. Click on the **[Add]** button to add a new Fax destination.
6. Enter the required fax number in the **[Add Fax Number]** box within the Fax Recipients section.
7. Click on the **[Add]** button.
8. **[Delayed Send]** can be selected in the **Delivery** box in **Fax Distribution List** if you want to send the fax at a specific time.
9. Click on the **[Apply]** button to accept the changes.

Document Management Fields (Optional)

This area enables you to add data fields to the Default Template. This information is filed with your scanned documents in the Job Log. The Job Log can then be accessed by third party software and the Document Management Fields information retrieved and associated with the scanned files.

The following fields are available. Click the underlined links for further information.

Field Name

This defines a name for the Document Management data that is to be associated with the scanned job. This value is not shown at the device user interface screen and is used by third party software to access the Document Management information. It can be up to 128 characters in length. This field cannot be left blank.

Field Label

If you would like the user to be able to modify the value of the Field Name select **[Editable]** next to 'User Editable'. Enter a value in the **[Field Label]** field. The label should identify the purpose of this field to the user.

Select **[Not Editable]** if the user can not change the Document Management Field's value. The user will not be presented with this Document Management Field at the device and the Default Value will be used.

Default Value

This is an optional requirement. This value defines the actual data that is to be assigned to that particular scan job. This field can be created blank or the user may edit this value at the device user interface screen.

To add a new Document Management field

10. Click on the **[Add]** button in the Document Management Fields box.
11. Enter a name for the field and provide a label and default value if required.
12. Click on the **[Apply]** button to accept the changes.

Other Options

You can configure a variety of settings for your scanned images, including:

- **Advanced Settings**
- **Layout/Adjustment**
- **Filing Options**
- **Report Options**
- **Workflow Scanning Image Settings**
- **Compression Capability**

For further information click the **Help** button (at the top of the Internet Services screen).

1. To change the settings click **[Edit]** in the appropriate area.
2. Select the appropriate options.
3. Click **[Apply]** to accept the changes.

Workflow Scanning Image Settings

The Workflow Scanning Image Settings screen allows you to create compressed image files for faster web viewing, and also to select Searchable options.

Note

Searchable options are only available when the Searchable File Formats service is enabled.

1. Click on the **[Edit]** button in the **Workflow Scanning Image Settings** area.
2. In the **Fast Web Viewing Options** area select **[Linearized PDF]** or **[Interleaved XPS]** if required. Linearized files allow single pages of a PDF to be displayed in a web browser before the entire file is downloaded. Interleaved XPS documents are also designed to be viewed quickly in a web browser. When a user views an interleaved XPS document, the document downloads and displays the text before the images so that the user can start reading the document without needing to wait for the whole document to download and display.
3. Select your required options for **Searchable XPS PDF and PDF/A Defaults**.
4. Click on the **[Apply]** button to accept the changes.

Compression Capability

1. Select **[Edit]**.
2. Select the required compression:
   - **CCITT Group 4**: uses Modified Read compression. Allows for fast scan and viewing performance but creates larger file sizes
   - **JBIG2**: JBIG2 will compress text smaller than Group 4 compression although it takes longer to process. JBIG2 exports PDF files as version 1.4 PDF
   - **Flate**: Select Flate if you want to add additional lossless compression to any JPEG compression performed by the device. Flate only applies to colour images within a Mixed Raster Content (MRC) file and exports files as version 1.4 PDF
   - **TIFF**: TIFF compression is available when the Colour Scanning Enablement Kit is fitted to the device. Some Windows applications cannot read the default TIFF output. If this functionality is required, select **[LZW]**. LZW is a lossless general purpose compression, used for colour and grayscale TIFF images. LZW creates a far larger file size than TIFF
   - **MRC**: If you want to use MRC Compression select the required option in the MRC Compression Capability area.
3. Click on the **[Apply]** button to accept the changes.

Apply Factory Defaults Settings

To restore the Default Template to its original settings click on the **[Apply Factory Default Settings]** button.

Note

This will delete any custom settings applied to the Default Template.

Set up Remote Template Pool Repository

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Click on the **[Advanced]** link.
8. Select **[Template Pool Setup]** in the directory tree.
9. For Protocol, use the drop-down menu to select the protocol you will be using to communicate with the template pool server.
10. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
11. Enter the **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the FTP location.
12. Type in the path to the location of the scan folder in **[Document Path]**. Enter the full path to the directory, starting at the root of FTP services. For example: */(directory name)/(directory name)*.
13. Select a radio button for **[Login Credentials to Access the Destination]**. Select **[System]** to have the system directly log in to the file server.

Supply remote server addressing and login credentials

- Referring to the on-line Help, in the upper right corner of the Internet Services screen, provide the network address to the remote server and the directory path on the server to the template files. Note that the format for a directory path for FTP is /directory/directory, while the format for a directory path for SMB is \directory\directory.
- Provide a Login (account) Name and (server) Password for the system to access the remote server. This is mandatory for use with a SMARTsend server. For information on creating accounts on the SMARTsend server, refer to the FreeFlow SMARTsend Installation and Administration Guide. Note that these accounts directly support the Login Source settings, accessed by clicking General under Workflow Scanning in Internet Services.

14. Enter a **[Login Name]** and **[Password]**, if the system will be directly accessing the file server.
15. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.

11 Scan to Home

The Scan to Home feature is supported through the Workflow Scanning service. Essentially, it is a template file (.xst) stored locally on the device, but in a different directory to the Workflow scanning templates or mailbox folders.

Users access the Scan to Home template by pressing the **[Workflow Scanning]** button on the Services screen of the user interface. The device queries LDAP to acquire the authenticated user's home directory, or appends the authenticated user's login name to a predefined network home path.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure the device is fully functioning on the network prior to installation.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.

  This is required to access Internet Services to configure Workflow Scanning. The Internet Services function is accessed through the embedded HTTP server on the device and allows System Administrators to configure scan settings by using an Internet browser.
- Workflow Scanning must be enabled on the Xerox device.
- Network Authentication must be configured on the Xerox device. The Authentication server and the server used to file scanned images must belong to same domain.

Additional Requirements for Scan to Home via LDAP Query

- A Windows 2000/2003 server with Active Directory Services (ADS) must be configured with LDAP Services and available on the network.
- The LDAP server information must be configured on the Xerox device.
- The user's Home Folder Location must be set on the ADS server. To verify the Home Folder Location, at the ADS server, go to [Administrator Tools] and then [Active Directory Users and Computers]. Select a user and select [Properties] and then [Profile]. Ensure the user's Home Folder Location is set. This will need to be set for each user who wants to use Scan to Home via LDAP Query.

Additional Requirements for Scan to Home with no LDAP Query

- Create a folder on your network where scans are to be filed. Share the folder and ensure users have Read and Write access privileges.

Enable and Configure Scan to Home

1. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Scan to Home]** link.
7. Select **[General]** in the directory tree.
8. On the **Scan to Home Setup** screen, check the **[Enabled]** checkbox for **Status**.
9. Optional step: In the **Friendly Name box**, type in a user-recognizable name of up to 127 characters for the template that will appear in Template Details on the device's user interface.
10. Optional step: if you want to change the default name of the Scan to Home template, enter the required name in the **[Template Name]** box. The default Scan to Home template is @S2HOME.

    Note

    If you change the default template name it is recommended that you enter a name that is easy to identify as the Scan to Home template, and enter a Friendly Name as mentioned in step 7. This will ensure users can identify the Scan to Home template. Templates can be created on the device by the Workflow Scanning, Scan to Mailbox and Scan to Home features with the same name.

11. In the **Determine Home Directory** area, select either **[LDAP Query]** or **[No LDAP Query]** to define the method that the device will use to find the user's home directory.

LDAP Query

12. Select **[LDAP Query]** if you want the device to query the LDAP server with the authenticated login name entered by the user to retrieve the user's home directory.
13. Verify the LDAP mapping for Home Directory is correct. To test it, click the **[LDAP Mapping for Home Directory]** link.
14. In the **LDAP - User Mappings** screen, in the **[Server Information]** area, check that the **LDAP Server** is set correctly for your environment.
15. In the LDAP screen click **[User Mappings]**. Enter a user name valid on your LDAP server, in the **[Enter Name]** area. Click **[Search]** and review the LDAP mapping for Home Directory. Return to the Scan to Home screen. Go to the Subdirectory instructions below.

No LDAP Query

16. Select **[No LDAP Query]** if you want to define a network path to file scanned images. The device will append the user's authentication login name to the end of the Network Home Path to create the user's home directory.
17. Enter the path to a location on your network where scans are to be stored in the **[Network Home Path]** area. The format should be: *servername**foldername*

Subdirectory

18. If you want the device to create a Subdirectory in the network home path, select **[Automatically create Subdirectory]** and enter a name in the **[Subdirectory]** name area.
19. If your network home path consists of folders with user names, and you want the device to file scanned images in these folders, select **[Append "User Name" to Path]**. The User Name refers to the name entered by the user when they are authenticated at the Xerox device.
20. If you selected No LDAP Query, you will need a method to distinguish individual ownership of job scans. To do this, select **[Append User Name to Path]**, or **[Automatically Create User Name directory to if one does not exist]**.
21. Click on the **[Apply]** button to accept changes.

Use Scan to Home

1. At the device touch the **[Workflow Scanning]** tab.
2. Enter your network authentication username and password.
3. At the Workflow Scanning Template List, touch the Scan to Home template. The default name is **[@S2HOME]**.
4. Put your documents in the device to scan and press the green start button.
5. Retrieve your documents from the home directory.

12 Scan to Mailbox

The Scan to Mailbox feature is supported through the Workflow Scanning option, purchased from your Xerox Sales Representative, and installed using a Feature Enablement Key. This feature provides the ability to scan to mailboxes in the device and then retrieve documents from the device using the web browser. This provides a convenient Workflow scanning feature for customers who do not wish to purchase and configure a separate networked server.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the device is fully functioning on the network prior to installation.
- Ensure Workflow Scanning is enabled on the device.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.
- Print a Configuration Report to verify that Workflow scanning (Scan to File) is an installed Option:
  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.

Enable Scan to Mailbox

1. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Scan to Mailbox]** link.
6. If necessary, select **[Enablement].**
7. Check the **[Enable Scan to Mailbox]** box.
8. Check the **[On Scan tab, view Mailboxes by default]** box.
9. Click on the **[Apply]** button.

Note

All Saved Jobs are stored as encrypted files if encryption of user data is enabled. Encryption ensures that third parties cannot read, print, scan and e-mail these files. You can enable / disable encryption of user data on the **User Data Encryption** page, see User Data Encryption on page 8-1.

Configure Scan to Mailbox

1. Click on **[Capacity]** in the directory tree to view the amount of hard drive space being consumed by files in Mailboxes.
   - **Capacity:** The total amount of space available on the device for scanned images.
   - **Used:** The space currently used to hold scanned images.
   - **Available:** The space left for scanned images
   - **Percentage Used**: The amount of space taken by scanned images as a percentage of the total space.
2. Click on **[Files]** in the directory tree to perform either an immediate or scheduled cleanup of folder files.

   The **Files** screen allows administrators to delete files stored in Scan to Mailbox folders.

   a. If you want to delete files now select the required option in the **Immediate Clear Up of All Folder Files** area and click on the **[Delete Files]** button.
   b. To schedule files to be deleted regularly, select the required option in the **[Schedule Clean Up of Folder Files]** area.
   c. Click on the **[Apply]** button.
3. Click on **[Folders]** in the directory tree. The Folders screen allows administrators to change folder passwords, delete folders or delete scanned images within folders.
   Dialog controls are self explanatory.
4. Click on **[Scan Policies]** in the directory tree. The Scan Policies screen allows administrators to set requirements for the use of passwords or folders. Check the required option:
   - **[Allow scanning to Default Public Folder]** - enable users to scan to the default Scan to Mailbox folder.
   - **[Require per job password for public folders]** - ensure users are required to enter a password at the device each time they scan to a public folder.
   - **[Allow additional folders to be created]** - allow users to create new folders.
   - **[Require password when creating additional folders]** - to create Private Folders, which require users to enter a password when they create a new folder.
   - **[Prompt for password when scanning to private folder]** - ensure users must enter a password at the device each time they scan to a Private Folder.
   - **[Allow access to job log data file]** - to be able to print the job log for specific scanned documents. The job log contains information about the scanned document. Third party applications can be used to search, file and distribute jobs based on their job log information. The job log can only be accessed for PDF or Multi-Page Tiff images.
5. Click on the **[Apply]** button.
6. When finished working with the dialogs, click on the **admin - Logout** in the upper right corner, and click on the **[Logout]** button.

   Note

   To see individual Mailboxes, click the Scan tab of Internet Services. To scan to these mailboxes, refer to the directions in the **Interactive User Guide** delivered with your device.

Use Scan to Mailbox

1. At the device touch the **[Workflow Scanning]** icon.
2. Touch your mailbox folder template in the Template Destinations List.
3. If prompted, touch the **[Enter Password for Folder]** button. Enter your mailbox folder password, touch **[Done]** and touch **[OK]**.
4. Touch the **[Options]** tab.
5. Touch **[File Format]**.
6. Select the required file format. Single-Page TIFF, PDF and Multi-Page TIFF are supported.
7. Touch **[Save]**.
8. Place a document on the device to scan and press the green start button.
9. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
10. Click the **[Scan]** tab
11. Select **[Mailboxes]**.
12. In the Scan to Mailboxes menu, select your mailbox.
13. If prompted, enter your mailbox folder password and click **[OK]**.
14. The scanned image will appear in the Folder Contents list. If it does not, click the **[Update View]** button.
15. If you selected to create a PDF or Multi-Page TIFF image, select the required option from the **[Action]** menu:
16. To save a copy of the image to your PC, select **[Download]** and click **[Go]**. Select a location on your PC to save the image.
17. To print the image at the device, select **[Reprint]** and click **[Go]**.
18. To delete the image select **[Delete]** and click **[Go]**.
19. If you selected job log on the Scan Policies screen you will see a **[Job Log]**. Select **[Open]** to view the job log or **[Save]** to save the job log to your computer.
20. If you selected to create a Single-Page TIFF image, select **[Open]** from the **[Action]** menu and click **[Go]**.
21. Select your Single-Page TIFF image from the list and select the required option from the **[Action]** menu. The options are **Download, Reprint** or **Delete**.
22. To remove all images from your mailbox, click the **[Delete All]** button.
23. To change your mailbox folder password or to remove your mailbox folder, click **[Modify Folder]**.
24. To change your mailbox folder password, enter your new password and click **[Save Password]**.
25. To remove your mailbox folder, click **[Delete Folder]**.

13 E-mail

The E-mail feature enables a user to scan paper documents into an electronic format and have those documents delivered to a set of e-mail recipients.

E-mail Addressing

Recipient addresses can be added by entering the SMTP (Simple Mail Transport Protocol) address, for example name@company.com, at the E-mail screen.

In addition, both an internal and a public address book can be configured for the device and accessed from the E-mail screen. Lightweight Directory Access Protocol (LDAP) provides access to the internal, or corporate, address book.

A public address book can be created from a list of names and addresses saved in a .CSV (comma separated values) file.

E-mail Authentication

Authentication (Service Access Control) can be enabled on the device to prevent unauthorized access to the network options. If Authentication is enabled a user will be prompted to enter a user name and password, or a PIN, before they can access the E-mail feature. For a full description of the Authentication feature refer to Authentication on page 7-1 of this guide. Authentication can be configured after E-mail has been installed.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure the device is fully functioning on the network prior to enabling E-mail.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional, so that the device web browser can be accessed. Ensure that DNS settings are configured on the device.

  This is required to access the device's Internet Services web pages, which can be used to configure E-mail settings from a network connected workstation's web browser.
- Obtain the IP Address of a functional SMTP mail server that accepts inbound mail traffic.
- Create an e-mail account on the mail server which the device will use as the default "From" address.
- Test the e-mail account by sending an e-mail from an SMTP mail client on a networked workstation. Use the new account name and password, if any to access the account and verify that e-mail was received.

Enable E-mail

Print a Configuration Report to verify that e-mail is enabled

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**

Verify or Configure your TCP/IP Domain Name (if necessary)

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Verify or re-configure the Domain for this device in the **[Domain Name]** box, (e.g.: abc.xyz.company.com). Note that it is preferable for the mail server to reside in the same domain as that of the device.

   Note

   If Dynamic Addressing has been set on the device (DHCP, DHCP/AutoNet, BootP or RARP) the Domain Name will not be accessible. If you need to change it, select **[Static]** from the **IP Address Resolution** drop down menu.

9. Click on the **[Apply]** button to implement any changes. If required, Click the **[Undo]** button to cancel any changes made and return to the previous values.

Configure an SMTP Server on the device

10. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
11. Click on the **[Properties]** tab.
12. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on **[Login]**.
13. Click on the **[Connectivity]** link.
14. Click on the **[Protocols]** link.
15. Select **[SMTP Server]** in the directory tree.
16. Under **Required Information**, select either **[IP Address]** or **[Host Name]**. Enter the **[IP Address]**, or the **[Host Name]** of the SMTP Server.
17. Enter a valid E-mail address in the **[ColorQube E-mail Address]** box (matching the account set up on the SMTP Server) which the device will use as a default E-mail From and Reply To address.
18. Under Optional Information, the **[Maximum Message Size]** (per fragment - the acceptable range is 512Kb to 20480 Kb), **[Number of Fragments]**, and the **[Total Job Size]** can all be set to control the size of E-mail jobs sent to the SMTP Server.
19. Select the required setting for the **[E-mail Job Splitting Boundary]**.

20. For Login Credentials, if the mail account does not need password access, select the **[None]** radio button.
21. If the mail account does require a password, select the **[System]** radio button, then enter the SMTP Server account name and password, where shown.
22. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on **[Login]**.
23. Click on the **[Apply]** button to implement any changes.

Configure General E-mail Settings

24. Click on the **[Services]** link.
25. Click on the **[E-mail]** link.
26. Select **[Defaults]** in the directory tree.

General

1. In the **General** area, click on the **[Edit]** button.
2. To change the e-mail **[From Address]**, enter a valid e-mail address.
3. Optional Step: Enter a **[From Name]**.
4. If LDAP is configured, select the required option next to the **[Allow Authenticated Users to Edit "From" Field when]**:
   - **[Address Book (LDAP) Search Successful]** - Users can edit the 'From' field when the LDAP server finds the user's address.
   - **[Address Book (LDAP) Search Failure]** - Users can edit the 'From' field when the LDAP server did not find the user's address.
   - **[Address Book (LDAP) Search Not Performed]** - Users can edit the 'From' field when the LDAP server has not been accessed.
5. Click on **[Yes]** next to **[Edit "From:" Field when Authentication is not Required]** if users can edit the 'From' field when authentication is not enabled on the device.
6. In the **[Message Body]** section, enter text that you want to appear as default in the body of e-mails sent from the device.
7. In the **[Signature]** entry box enter text that you want to appear as the default signature in every e-mail.
8. Select an option from the **[Confirmation Sheet]** drop-down menu:
   - **[Off]** - This setting will not produce a Confirmation Sheet.
   - **[On]** - This setting will produce a Confirmation Sheet that will provide error information and indication that the job has reached the recipient(s).
   - **[On Errors Only]** - This setting will produce a Confirmation Sheet only when error information is indicated.
9. Check the **[Enable]** box for **Auto Send to Self**, if you wish to add a copy of the sender's e-mail to the Address List.
10. The **Enable E-mail Security** feature provides enhanced security when sending e-mail messages and attachments. This feature utilizes the authentication options of the device, along with an optional secure e-mail server, to protect data transmitted as e-mail.
11. Click on the **[Apply]** button to implement changes and return to the **Default** page.

Scan to E-mail

Scan to E-Mail settings will set the defaults for the following: E-mail Subject, Output Color, 2-Sided Scanning and Original type.

1. Click on the **[Edit]** button.
2. Enter text in the **[Subject]** box to define a default subject that will appear in e-mails sent from the device.
3. Select the required option for **[Output Color]**.
4. Select the required content option for **[Content Type]**.
5. Select the required scanning option for **[2-Sided Scanning]**.
6. Select the option that best describes the **[How Original was Produced]** of your e-mail documents.
7. Select the required option for **[Scan Presets]**.
8. Click on the **[Apply]** button to accept the changes.

Advanced Settings

Advanced settings allows you to select options as follows:

- **Image Options** - allows you to lighten or darken the image to be scanned.
- **Image Enhancement** - prevents reproduction of unwanted shading from the originals.
- **Resolution** - allows you to choose the resolution setting to be applied to the scan.
- **Quality/File Size** - allows you to choose the quality setting for the document or image to be scanned and mail.

1. In the **[Advanced Settings]** area, click on the **[Edit]** button.
2. Select the required options in the **[Advanced Settings]** area.
3. Click on the **[Apply]** button to implement changes and return to the **Default** page.

Layout Adjustment

Layout Adjustment settings includes:

- **Original Orientation** - allows you to choose the direction your images are loaded in the Document feeder.
- **Original Size** - allows you to choose either **[Auto Detect]** which allows the device to automatically detect the original size of the document, or **[Manual Input Size]** which requires user to input the size of the document.
- **Edge Erase** - when selected allows scanning the complete page.

1. In the **[Layout Adjustment]** area, click on the **[Edit]** button.
2. Select the required options.
3. Click on the **[Apply]** button to accept changes and return to the **Default** page.

Filing Options

Filing options allow you to specify the default e-mail file format. There are two options:

- **File Format** - allows user to select the format of the document from either TIFF, mTIFF, JPEG, PDF, PDF/A or XPS.
- **Searchable Options** - allows user to select searchable option of searching either Image Only or Searchable Languages.

1. In the **[Filing Options]** area, click on the **[Edit]** button to specify the default file format options.
2. Click on the **[Apply]** button to implement changes and return to the **Default** page.

E-mail Image Settings

Image Settings allow you to select linearized PDF and interleaved XPS images for faster web viewing.

Note
Searchable options are only available when the Searchable File Formats service is enabled.

Email Image Settings allow you to specify the e-mail Image Settings. There are two options:

- **PDF & PDF/A Settings** - allows you to select Optimized for Fast Web Viewing.
- **Searchable XPS PDF & PDF/A Defaults** - allows you to select the Searchable Options and Text Compression Setting (PDF & PDF/A only).

1. In the **[E-mail Image Settings]** area, click on the **[Edit]** button to create compressed image files for faster web viewing, and also to select Searchable options.
2. Click on the **[Apply]** button to implement changes and return to the **Default** page.

Configuring Public and Internal Address Books (LDAP)

The device supports two types of address book:

- **Internal** - A global address book provided by LDAP (Lightweight Directory Access Protocol) services.
- **Public** - An address book created from a list of names and addresses saved in a **.CSV** file (comma separated values) file.

Both address book types can be configured for use on the device at the same time.

Addressing - Internal Address Book (LDAP)

Note
LDAP support is only available on the device. Configuration of the LDAP directory settings requires the network to support LDAP services.

For LDAP Addressing, see LDAP Addressing on page 13-6.

For Public Address book, see Create a Public Address Book on page 13-9.

LDAP Addressing

LDAP (Lightweight Directory Access Protocol) is a popular protocol used by large accounts to access large quantities of data including corporate address books. The local system will need to know where the LDAP server is located on the network and may need a login name and password if the LDAP server is not configured to allow NULL names and passwords.

The Internet Services **LDAP** page enables you to configure Lightweight Directory Access Protocol information.

LDAP is used for the following activities:

- To access the corporate address book to locate e-mail addresses for use with the E-mail and Internet Fax services
- To authenticate users when configured as the method of Authentication
- To authorize users to gain access to device features, when configured as the method of Authorization.

For instructions on how to configure Authentication and Authorization, see Authentication on page 7-1.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the E-mail feature is functional on the device and your network supports LDAP services.
- Obtain the IP Address of your LDAP Server. The device may also need a login name and password if the LDAP server is not configured to allow NULL names and passwords.
- Use an LDAP client to validate your settings before inputting them into the Internet Services menus. LDAP clients include Microsoft Outlook Express, Microsoft Outlook and Netscape Communicator.
- To use host names, DNS must be configured on the device.

At your Workstation

1. Open your web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[LDAP]** in the directory tree.
8. In **Server Information** area select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button and enter the **IP Address** and **Port** or the **Host Name** and **Port** of the LDAP Server.
9. Select the server type from the **[LDAP Server]** drop down menu.
10. Enter any further information, as required, in the **Optional Information** area.
    - **Search Directory Root** allows you to limit the LDAP search by entering the location on the server where the LDAP information is stored.
    - **Login Credentials to Access LDAP Server**: Select the **[None]** radio button if no login is required. If you select **[Authenticated User]** the device will use the login details entered by the user to access the LDAP server. This option requires Authentication to be configured on the device. If **[System]** is selected the device will specify the LDAP server login details and enter the required

information in the **[Login Name]** and **[Password]** boxes. Format for the login name may be login name or domain/login name.

- **Enter a Login Name** and **Password**, if required, for the device to access the LDAP server. Format for the login name may be login name or domain/login name.
- **SSL**: If SSL is required, check the **[Enable]** box.

  Note
  SSL requires a server certificate to be available to the device.

- If you want the device to verify that the server certificate is trusted, valid and has a fully qualified domain name (FQDN), check the **[Validate Repository SSL Certificate]** box.

  Click on the **[View Trusted SSL Certificates]** link to view secure certificates that have been uploaded to the device. (Click the browser **[Back]** button to return to the LDAP Settings screen).
- **Maximum Number of Search Results** (between 5 and 100). This is the maximum number of addresses that will appear which match the search criteria selected by the user. Set the search results to one less than the server will allow. For example, if the LDAP server limit is 75, set the search results to 74 or less.
- **Search Timeout:** There are two options. You can let the server use its timeout limit by selecting the [Wait LDAP Server Limit], or specify how many seconds the search should last (between 5 and 100). If the search takes longer than the time specified in the [Wait... seconds] box the user will be notified that the search failed.
- **[LDAP Referrals]:** if the primary LDAP server is connected to additional servers, the search will continue on those servers as well.
- The **Perform Query on option** will help control the returns by allowing the LDAP query to be on **[Mapped Name]** or **[Surname and Given Name Fields]**. Netscape and Lotus Domino will typically require a setting of Surname to allow returns of "lastname, firstname".

11. Click on the **[Apply]** button to implement the changes.

Contexts

12. Click on the **[Contexts]** tab under the LDAP title at the top of the screen.

    Contexts are used with the Authentication feature. The administrator can configure the device to automatically add an authentication context to the Login Name provided by a user.
13. Enter information in the **[Default Login Context]** box.
14. Click on the **[Apply]** button.

User Mappings

Fields contained within LDAP structures are not standardized. This section allows you to find out what results you will get when searching for a name using one of the LDAP servers. Choosing the right LDAP server will improve your success when performing name searches.

To map the LDAP fields:

15. Click on the **[User Mappings]** tab in the LDAP Settings Menu at the top of the screen.
16. Click on the **[Search]** button.
17. The information about this user is then displayed against the fields shown on the device. By using the drop down menu under **Imported Heading** boxes re-map any fields you require against the device's properties.

Note

Internet Fax users should ensure that the **Internet Fax** field is NOT set to **"No Mappings Available"** in the drop down menu. This setting will prevent the LDAP Address Book appearing on the Internet Fax screen at the device. Select **[Mail]** as the Internet Fax setting.

18. When you have finished making your selections click on the **[Apply]** button.

At the Device

19. Select the **[E-mail]** button, then touch **[OK]**.
20. Touch **[Address Book]**.
21. Enter a name using the keyboard touch screen, for example: lastname, firstname.
22. Touch **[Search]**. The Search Results Screen will appear. Select the required name from the list (if there is more than one match).
23. Touch the **[To]:** button to select the name as a recipient for your e-mail.
24. Touch **[Close]**. The e-mail address will appear in the Address List.
25. Place a document to e-mail in the document handler and press the green start button.
26. Verify that the recipient received the scanned document in his/her e-mail inbox.

Configuring the 'From' Address

For 'From' address configuration refer to the E-mail Settings screen within Internet Services. For instructions review the Configure General E-Mail Settings section earlier in this document.

You have completed the steps to configure a company address book via LDAP.

Addressing - Public Address Book

If you do not have an LDAP server to provide access to a corporate address list, the device will accept a Public Address Book file that contains a list of user names and associated e-mail addresses. This file must be in a CSV (Comma Separated Values) format for the device to be able to read the file contents. The device can have access to both an LDAP server and a public address book. If both are configured the user will be presented with the choice to use either address book to select e-mail recipients.

The majority of word processing or spreadsheet packages will allow you to create a CSV file. A selection of E-mail applications will also allow you to export a list of users in the CSV file format. There are also several conversion packages available on the web.

Public Address Book

The Internet Services Public Address Book screen allows you to upload a list of names and e-mail addresses which can be accessed via the Public Address Book at the device.

The Public Address Book consists of a text file a CSV (Comma Separated Values) format. The majority of word processing or spreadsheet packages will allow you to create a CSV file. A selection of E-mail applications will also allow you to export a list of users in the CSV file format. There are also several conversion packages available on the web.

The E-mail or Internet Fax services must be enabled at the device to access the Public Address Book.

Create a Public Address Book

1. Open an application that supports CSV files (for example, Microsoft Excel).
2. Create a list of addresses with the following headings: name and address.

   For example:

Name	Address
name	firstname.lastname@company.com
name2	firstname.lastname@company.com
name3	firstname.lastname@company.com

   The order in which entries are displayed in the Public Address Book at the device will depend on how the entries are sorted in the CSV file.
3. Save the file as a CSV (comma separated values) file with the extension .csv.
4. We recommended that you keep a copy of the .CSV file once created.

At your Workstation

5. Open the web browser, enter the *IP address* of the device in the Address bar, and press **[Enter]**.
6. Click on the **[Properties]** tab.
7. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
8. Click on the **[Login]** button.
9. Click on the **[Services]** link.
10. Click on the **[E-mail]** link.
11. Select **[Public Address Book]** in the directory tree.
12. Click on the **[Browse]** button and browse to the location of the Address Book File **(*.CSV)** created step 3, above.
13. Highlight the **.CSV** file and click **[Open]** in the Choose File window.
14. Click on the **[Import Now]** button in the web browser. If an address book is already in existence, you will be warned that the new import will overwrite the existing address book.
15. Or you can use the **[Map Existing Address Book]** button to map to an existing Address Book.
16. Click on the **[OK]** button to import the Address Book.
17. Click on the **[Apply]** button.

    Note

    If an address book is already established, you may be warned that duplicate entries exist and the new entries will be ignored.

At the Device

18. Select the **[E-mail]** button, then touch **[OK]**.
19. Touch **[Address Book]**.
20. Touch **[Public]** in the Address Books drop-down list.
21. Enter the name of the recipient of your e-mail.
22. Touch **[Search]**.
23. The public address book appears. Select the required name from the list.
24. Touch the **[To]:** button.

25. Touch **[Close]**.
26. Place a document to e-mail in the document handler and press the green start button.
27. Verify that the recipient received the scanned document in his/her e-mail inbox.

You have completed the steps to create a public address book.

14 Internet Fax

Internet Fax allows you to send documents to one or more Internet Fax destinations, and receive an Internet Fax at the device without requiring a telephone connection.

The Internet Fax service provides confirmation of delivery in much the same way as for the standard Fax service, by returning the Delivery Status Notifications (DSN's) and Message Disposition Notifications (MDN's) for the job via the Internet.

Using Mixed Size Originals

It is recommended that the originals used with the Internet Fax feature are of the same size. If mixed sized originals are to be used ensure that the Mixed Sized Originals option is selected when performing an Internet Fax at the device. Once the Internet Fax feature has been configured, select the **Internet Fax** tab at the device, followed by **Image Adjustment** and then **Original Input**. **Mixed Sized Originals** can be selected as an option.

Internet Fax Addressing

Recipient addresses can be added by entering the SMTP (Simple Mail Transport Protocol) address, for example *name@company.com*, at the Internet Fax screen.

In addition, both an internal and a public address book can be configured for the device and accessed from the Internet Fax screen. Lightweight Directory Access Protocol (LDAP) provides access to the internal, or corporate, address book.

A public address book can be created from a list of names and addresses saved in a .CSV (comma separated values) file.

Internet Fax Authentication and Authorization

Authentication (Service Access Control) can be enabled on the device to prevent unauthorized access to the network options. If Authentication is enabled a user will be prompted to enter a user name and password, or a PIN, before they can access the Internet Fax feature. For a full description of the Authentication feature refer to Authentication on page 7-1 of this guide. Authentication can be configured after Internet Fax has been installed.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure the device is fully functioning on the network prior to enabling Internet Fax.
- Install the Scanning Hardware Kit.

  Refer to the instructions contained with the Workflow Scanning/E-mail Kit to complete this task. Contact your Xerox Sales Representative if you do not have the Scanning Hardware Kit.
- Ensure TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 2-5.

  This is required to access the device's Internet Services web pages, which can be used to configure Internet Fax settings from a network connected workstation's web browser.

  For instructions on how to configure TCP/IP and HTTP refer to Configure Protocols with Internet Services on page 2-9.
- Obtain the IP Address of a functional SMTP (Simple Mail Transport Protocol) mail server that accepts inbound mail traffic.
- Ensure that DNS settings are configured on the device.
- Obtain the IP Address, account and password details of a POP3 (Post Office Protocol 3) Mail Server.
- Create an e-mail account which the device will use as the Internet Fax "From" address.
- Test the e-mail account by sending an e-mail from a networked workstation running SMTP and POP3 clients. After sending the e-mail, log in to the POP3 server to verify receipt of same.

Enable Internet Fax

Print a Configuration Report to verify that Internet Fax is an Installed Option.

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**

Configure a Domain Name and SMTP Address

Note

A domain name must be entered to enable configuration of the Internet Fax feature.

To Configure a Domain Name

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.

7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Enter the domain name in the **[Domain Name]** box, (e.g.: abc.xyz.company.com).

   Note

   If Dynamic Addressing has been set on the device (DHCP, DHCP/AutoNet, BootP or RARP) the Domain Name will not be accessible. If you need to change it, select **[Static]** from the IP Address Resolution menu list, and click on the **[Apply]** button.

9. Click on the **[Apply]** button to implement any changes.

   Note

   It is only necessary to configure the DNS settings if Host Names are to be used.

Configure an SMTP Address

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[SMTP Server]** in the directory tree.
8. Under **Required Information**, select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**. Enter the **[IP Address]**, or the **[Host Name]** of the SMTP Server.
9. Enter a valid E-mail address in the **[ColorQube E-mail Address]** box (matching the account you set up for this device on the SMTP Server).
10. Under **Optional Information**, the **[Maximum Message Size]** (per fragment - the acceptable range is 512Kb to 20480 Kb), **[Number of Fragments]**, and the **[Total Job Size]** can all be set to control the size of E-mail jobs sent to the SMTP Server.
11. Select the required setting for the **[E-mail Job Splitting Boundary]**.
12. For Login Credentials, select **[None]** if the mail account does not need password access.
13. If the mail account does require a password, select **[System]**, then enter the SMTP Server **Login Name** and **Password**.
14. Select the required option for **[Logo Credentials for the Walkup User to send Scanned E-mails**.
15. Click on the **[Apply]** button to implement any changes.

Configure POP3 Settings

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[POP3 Setup]** in the directory tree.
8. Select either **[IPv4 Address]** or **[Host Name]** and enter the POP3 Server IP Address and Port number or Host Name and Port number in the **Server Information** section.
9. Enter the **[Login Name]** and **[Password]** details.

10. Check the **[Enable receipt of E-mail by POP3]** box in the **POP3 Settings** section.
11. Enter the required setting for the **[Polling interval]** (1-60 minutes).
12. Click on the **[Apply]** button to implement any changes.

Configure General Internet Fax Settings

13. Click on the **[Services]** link.
14. Click on the **[Internet Fax]** link.
15. Select **[Defaults]** in the directory tree.
16. Also in the **General** section, enter the time required for the **[Delivery Confirmation Timeout]** (0-72 hours).
17. In the **[Message Body]** box, enter a default message that will appear on received internet faxes. Check the required boxes to select the information fields that will be automatically displayed in the body of the internet fax message.
18. In the **[Signature]** box, enter any additional information you would like included on any fax sent from the device.
19. From the **[Confirmation Sheet]** drop-down menu, select the required setting for printing a confirmation sheet.
20. In the **Filing Options** section, click on the **[Edit]** button. Make desired changes to the **[Document Format]** and **[Acknowledgement Report]**.
21. Click on the **[Apply]** button to implement changes and return to the **Default** page.
22. In the **Internet Fax Image Settings** section, click on the **[Edit]** button, then enter a subject that will appear in all outgoing internet fax messages, and click on the **[Apply]** button to implement changes and return to the **Default** page.
23. In the **Advanced Settings** and **Layout Adjustment** sections, click on the **[Edit]** button, set desired parameters, and Click on the **[Apply]** button to implement changes and return to the **Default** page.

Internet Fax Receive Settings

24. Click **[Internet Receive Settings]** in the directory tree.
25. In the **Filter Options** section check the **[Accept E-mail with no attachment]** box, if required.
26. Check the boxes according to the file types of attachments that can be accepted under the **[Accept the following attachments]**.
27. In the **Finishing Options** section select the required setting from the drop-down menu for **[Stapling]** and **[2-Sided Printing]** drop down menu.
28. In the **[Receipt Options]** section, check the **[Send Confirmation reply when requested (allow device to send MDN)]** box, if required.
29. Check the **[Print Cover Sheet with incoming E-mail messages]** box, if required.
30. Click on the **[Apply]** button to implement any changes, and click on **[OK]**.

At the Device

31. Press the **[Services]** button, touch the **[Internet Fax]** icon.
32. Touch **[New Recipient]** button, then touch **[To]**: button.
33. Enter an internet fax recipient address.
34. Touch the **[Add]** button, then touch **[Close]**. The e-mail address will appear in the Address List.
35. Place a document to fax in the document handler and press the **[Start]** button.
36. Verify the recipient receives the document at the internet fax address.

The 'From' Address

The Internet Fax 'From' address is the e-mail Address entered for the device when the POP3 address details were configured and is not an editable field.

Receipt of Internet Fax Messages

Verify the device can also receive Internet Fax messages. To do this touch the **[Internet Fax]** button, touch the **[To]** button and enter the e-mail address configured for the device. Touch the **[Add]** button. Place a document in the document handler and press the green start button. The document should be received and printed as an Internet Fax job.

Internet Fax Addressing

Once configured, an internal and a public address book can be accessed when using the Internet Fax feature at the device. Lightweight Directory Access Protocol (LDAP) provides access to the internal (corporate) address book.

A public address book can be created from a list of names and addresses saved in a .CSV file (comma separated values) file. Both address book types can be configured for use on the device at the same time.

15 Embedded Fax

Embedded Fax enables users to send hard copy documents to another fax device (or multiple fax devices) via a telephone connection. The Embedded Fax option requires a fax card to be fitted to the device and connected to a telephone line. When you install the fax card and power on the device, the Fax Setup window will appear on the screen with step by step instructions to lead you through the configuration. The Fax Setup procedure can be undertaken immediately following installation of the fax card, or at a later date.

Embedded Fax is an optional feature for the device.

Server Fax and Embedded Fax

The Embedded Fax and Server Fax services are mutually exclusive and only one of them can be enabled at any time. If Server Fax is currently enabled and Embedded Fax is then enabled, Server Fax will be disabled automatically.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure the device is fully functioning in its existing configuration prior to installation.
- Ensure the device has access to a telephone connection.
- Obtain the telephone number that you wish to assign to the fax device.

Hardware

- Locate the Fax Hardware Kit. Contact your Xerox Sales Representative if you do not have the Fax Hardware Kit.
- Locate the 2 Line Fax Kit if this has been purchased.

Install the Fax Hardware Kit

Note

If Server Fax is installed on the device when the Embedded Fax Install Wizard is running, the Server Fax feature will be disabled and users will only have access to the Embedded Fax feature.

1. Switch the power off by pressing the **[Power Off]** button.
2. Wait until the Network Controller to fully power off. The blinking green network activity light will be extinguished when this occurs.
3. Install the Fax Hardware Kit following instructions contained with the kit.
4. Connect the telephone cable to the port on the device.

5. If you have purchased the 2 Line Fax Kit, fit the kit following the instructions contained with the kit. Once fitted, connect the second telephone cable to the second port on the back of device.
6. Switch the device on by pressing the **[Power On]** button.

Complete the Fax Setup Screens

1. The Fax Setup (or Install) screen should appear. If it does, touch **[Set up Now]** If it does not, see Deferred Fax Setup later in this document.

   Note

   If you do not wish to run through the fax configuration, touch the **[Set up Later]** button. Embedded Fax will be unavailable until the fax configuration screens are completed from within the administrator tools screens. See Deferred Fax Setup later in this document, for instructions.

2. Select the required (or nearest) country location by touching an entry in the **[Country Setup]** list.
3. Touch **[Next]**.
4. Touch **[Line 1]** or **[Line 2]** if applicable.
5. The Line Configuration screen appears. Select the required dialing method. For a tone line select **[Tone]**. For a 10 pulse per second line select **[Pulse]**. If in doubt, touch **[Tone]**.

   Note

   The Pulse/Tone feature is not available in some countries.

6. Enter the fax telephone number for the device by touching the **[Fax Phone Number]** button and pressing the buttons on the keypad. At least two digits must be entered here.

   Note

   Customers in the Czech Republic are advised to contact their Xerox Service Representative to perform this task.

7. Optional step: enter a Line Name for the device by touching the Keyboard icon and touching the characters. A maximum of 30 characters may be entered.
8. Touch **[Save]**.
9. Touch **[Next]**.
10. The **[Line Settings]** window appears. Select the required option for the line by touching one of the buttons as follows:

    [Send and Receive]: the device is capable of sending and receiving fax transmissions.

    [Send Only]: the device is only capable of sending faxes.

    [Receive Only]: the device is only capable of receiving faxes.

11. Touch **[Next]**.
12. Touch **[Save]** to exit the Line Setup Complete screen.
13. Touch **[Save]** to save the Fax Install Complete screen.

    The device will reboot with the new settings.

14. Test the fax connection by sending a fax document. Press the **[Services]** button.
15. Touch the **[Fax]** icon button.
16. Enter the number of a nearby fax device using the keypad and touch the **[Add]** button.
17. Place your documents in the document handler and press the **[Start]** button.
18. Verify that your documents are received at the other fax device.

You have completed the embedded fax setup.

Configure Fax Settings

This procedure is only necessary if you have not yet configured the fax settings, or if you have already fitted the fax card and wish to change any settings for the fax option.

At the Device

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Fax Service Settings]**.
6. Touch **[Line 1 Setup]** or **[Line 2 Setup]**.
7. The Line 1 (or 2) Setup screen appears.
8. Select the required **[Dial Type]**. For a tone line select **[Tone]**. For a 10 pulse per second line select **[Pulse]**. If in doubt, touch **[Tone]**.

   Note

   The Pulse/Tone feature is not available in some countries.

9. Touch the **[Fax Number]** button and enter the device's fax number by using the keypad.

   Note

   Customers in the Czech Republic are advised to contact their Xerox Service Representative to perform this function.

10. Optional step: enter a Line Name for the device by touching **[Line Name]** and using the on-screen keyboard to enter a maximum of 30 characters.
11. Select the required option for the line by touching one of the buttons as follows under **[Options]**:

    [Send and Receive]: the device is capable of sending and receiving fax transmissions.

    [Send Only]: the device is only capable of sending faxes.

    [Receive Only]: the device is only capable of receiving faxes.
12. Touch **[Save]** to exit the Line Setup screen.
13. Touch **[Log In / Out]** to exit the Tools pathway and the device will reboot with the new settings.

You have completed the steps. For detailed information about other embedded fax features, refer to the Training and Information CD2 delivered with your device.

Deferred Fax Setup

This procedure is only necessary if you pressed the Setup Later button when the Fax Setup screens appeared and you now wish to configure Embedded Fax settings using the Fax Setup Screens.

At the Device

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Fax Service Settings]**.

6. Touch the **[Fax Country Setting]**
7. Select the required (or nearest) country location by touching an entry in the **[Country Selection]** list.
8. Touch **[Save]**.
9. Touch **[Line 1]** or **[Line 2]** Setup.
10. The Line 1 Setup screen appears.
11. Select the required Dial Type. For a tone line select **[Tone]**. For a 10 pulse per second line select **[Pulse]**. If in doubt, touch **[Tone]**.

    Note

    The Pulse/Tone feature is not available in some countries.

12. Enter the fax telephone number for the device by touching the **[Fax Number]** button and pressing the buttons on the keypad. At least two digits must be entered here.

    Note

    Customers in the Czech Republic are advised to contact their Xerox Service Representative to perform this task.

13. Optional step: enter a Line Name for the device by touching **[Line Name]** and using the on-screen keyboard to enter a maximum of 30 characters.
14. Select the required option for the line by touching one of the buttons as follows under **[Options]**:

    [Send and Receive]: the device is capable of sending and receiving fax transmissions.

    [Send Only]: the device is only capable of sending faxes.

    [Receive Only]: the device is only capable of receiving faxes.
15. Touch **[Save]** to exit the Line Setup screen.
16. Touch **[Log In / Out]** to exit the Tools pathway and the device will reboot with the new settings.
17. Test the fax connection by sending a fax document. Press the **<Services>** button.
18. Touch the **[Fax]** icon.
19. Enter the number of a nearby fax device using the keypad.
20. Place your documents in the document handler and press the **<Start>** button.
21. Verify that your documents are received at the other fax device.

You have completed the embedded fax setup. For detailed information about other embedded fax features, refer to the Training and Information CD2 delivered with your device.

16 LAN Fax

LAN (Local Area Network) Fax enables users to send documents to fax devices directly from their computers. Once enabled, users select the Fax option from their printer driver. The LAN fax option requires the Embedded Fax Kit to be fitted to the device.

Information Checklist

Make sure that you have installed the Embedded Fax as stated in the Embedded Fax section of this guide before continuing with this procedure.

> Note
> If Server Fax is enabled, Embedded Fax will be disabled and the LAN Fax option will be unavailable in the driver.

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure that the device is fully functioning in its existing configuration.
- The Embedded Fax option must be installed on the device.
- The ColorQube printer driver must be installed on your Workstation.

Enable LAN Fax (Windows Printer Drivers)

LAN Fax must be enabled in your printer driver to support the LAN fax feature. LAN fax can be enabled automatically, with Bi-directional communication or manually. Both instructions are detailed below.

Configure the Printer Driver - Automatically

At your Workstation

1. From the **[Start]** menu click on:
   - **[Printers and Faxes]** - Windows XP. If you cannot see this option in the **[Start]** menu, then click on **[Start]**, followed by **[Control Panel]** first.
   - **[Settings]** then **[Printers]** - Windows 2000
   - **[Settings]** then **[Printers and Faxes]** - Windows 2003
2. Right-click on your printer driver and click on **[Properties]**.
3. Click on the **[Configuration]** tab.
4. Click on **[Bi-Directional Setup]**.

5. Enter the IP Address of your printer, if necessary.
6. Ensure **Bi-directional Communication** is set to **[Automatic]**, or click on **[Manual]** and enter the Device Name or IP Address. Click on **[OK]**.
7. Click on the **[Installable Options]** button.
8. Ensure that LAN Fax shows a status of **[Installed]**.
9. Click on **[OK]**.

Configure the Printer Driver - Manually

To configure the printer driver without using bi-directional communication return to the Configuration tab within the Properties of the printer driver.

1. Click on **[Installable Options]**.
2. Click on the **[LAN Fax]** menu.
3. Click on **[Installed]**.
4. Click on **[OK]**.
5. Click on **[OK]** to close the printer driver Properties.

Use the Feature

Windows: At your Workstation

1. Open a document that you want to fax.
2. Click on **[File]** then **[Print]**.
3. Click on your printer.
4. If you have a **[Properties]** or **[Preferences]**, click on it.
5. Check that you are on the **[Paper/Output]** tab.
6. Click on the **[Job Type]** menu.
7. Click on **[Fax]**. Follow the steps in ***Add Fax Recipient*** below.

Mac OS Users

1. Open a document to fax and click on **[File]** and then **[Print]**.
2. Click on the *Xerox* printer.
3. Click on **[Xerox Features]** from the **[Copies and Pages]** menu
4. Ensure you are in the **[Paper/Output]** area and click on the **[Job Type]** menu.
5. Click on **[Fax]**.

Add Fax Recipient

1. Click on **[Add Fax Recipient]**.
2. Enter the name of the fax recipient in the **[Name]** area.
3. Enter the fax number of the recipient in the **[Fax Number]** area.
4. Enter details such as Organization, Phone Number, E-mail Address and Mailbox number if required.
5. If you want to add this recipient to your personal phonebook, click on **[Add to Personal Phonebook]**.

6. Click on **[OK]**.
7. The recipient will show in the **[Recipients]** list.

Add Recipient from Phonebook

8. If you have a Personal Phonebook created you can add a recipient name from it. Click on **[Add from Phonebook]**. Otherwise, go to step 17.
9. In the **[Add from Phonebook]** menu, if you have more than one phonebook available, select the required phonebook from the **[Personal Phonebook]** menu.
10. Click on the recipient that you want to fax to. To view the details for the recipient, double-click on the recipient.
11. If you want to add more than one recipient, hold down the **[Ctrl]** key on your keyboard and click on each name.
12. When you have finished selecting your recipients, click on the green arrow. The names appear in the **[Fax Recipients]** list.
13. Click on **[OK]**.
14. If you want to save this list of names as a group, click on the **[Save As Group]**.
15. Enter a name for your group in the **[Group Name]** box.
16. Click on **[OK]**.

Setting up a Cover Sheet

17. Click on the **[Cover Sheet]** tab.
18. If you want to add a cover sheet to your document, click on **[Print a Cover Sheet]** from the **[Cover Sheet Options]** menu.
19. Enter the information that you want to show on the cover sheet in the **[Cover Sheet Options]** box.
20. If you want to add a graphic or logo to the cover sheet (a .bmp, .gif or .jpeg), click on **[New]** from the **[Cover Sheet Notes]** area.
21. To add a graphic or logo, click on **[Picture]** from the **[Options]** menu.
22. Click on **[Choose File]** then click on the required graphic or logo from your Workstation.
23. Click on the required settings to adjust the scale, position and preview options of your graphic.
24. Click on **[OK]**.
25. Click on the **[Cover Sheet Image]** menu and click on **[Options]**:
    - Click on **[Print in Background]** to print the graphic behind any text on the cover sheet.
    - Click on **[Print in Foreground]** to print the graphic at the front of your cover sheet or click on **[Blend]** to print a faint image of the graphic.
26. Click on the required **[Cover Sheet Paper Size]**.
27. Click on **[OK]**.

Setup Fax Options

28. Click on the **[Options]** tab.
29. Click on the required option from the **[Confirmation Sheet]** drop-down menu.
30. Click on the required speed from the **[Send Speed]** drop-down menu.
    - **G3 (14.4 Kbps)** - Selects the transmission rate based on the maximum capabilities of the receiving fax device. Initial transmission speed will be 14,400 Bits Per Second (bps). This rate minimizes transmission errors by using Error Correction Mode (ECM).

- **Super G3 (33.6 Kbps)** - This is the fastest transmission rate and is the default setting. This rate minimizes transmission errors by using Error Correction Mode (ECM). Initial transmission speed will be 33,600 Bits Per Second (bps).
- **Forced 4800 bps** - Used in areas of low quality communication, when experiencing telephone noise, or when fax connections are susceptible to errors. 4800 bps is a slower transmission rate but is less susceptible to errors.In some regional areas, the use of 4800 bps is restricted.

31. Click on the required resolution from the **[Fax Resolution]** drop-down menu.
32. If you want to send your fax at a specific time, click on the **[Send At:]** and enter the time in the next 24 hours that you want the device to send your fax.
33. If your telephone system requires Fax users to enter a prefix in front of fax numbers, click on the **[Dialling Prefix]** checkbox and enter the prefix in the box.
34. If your call requires a Charge Code number for billing purposes, click on **[Credit Card]** checkbox and enter the details for the charge code in the box.

Setup Phone book Preferences

35. Click on **[Preferences]**.
36. If you have more than one phonebook configured, you can specify which phonebook to use as the default from the **[Default Phonebook]** menu.

Personal Phonebook

The Personal Phonebook is created when you add fax numbers on the **[Fax Recipients]** tab. The Personal Phonebook is automatically saved to your PC to a file called default.pb. To view the Personal Phonebook, click on the **[Select File...]** next to Personal Phonebook, select and open the **[default.pb]** file. Click on **[Open]** next to Personal Phonebook on the Preferences tab.

Shared Phonebook

The Shared Phonebook is a list of fax numbers and recipient details that has been saved to a network drive for more than one person to use. To access a shared phonebook:

1. Click on the **[Select File...]** next to Shared Phonebook and locate the **[default.pb]** shared phonebook file on your network.
2. Click on **[Open]** next to Shared Phonebook to view the phonebook.

User Preferences

3. If you want to be notified when you add duplicate recipients to the phonebook, select the **[Prompt When Adding Duplicate Recipients]** option.
4. If you want to be notified when you delete a recipient from the phonebook, select the **[Prompt When Removing a Recipient]** option.
5. If you want to always use the Current Recipient List, click on the **[Always Use Current Recipient List]** checkbox.
6. If you want to use the current Cover Sheet notes, click on the **[Always Use Current Cover Sheet Notes]**.
7. Click on **[OK]** when you have finished making your selections.
8. Click on **[OK]** to close the **[Fax]** window.
9. Click on **[OK]** on the **[Paper/Output]** tab to send your fax. The document will fax with the specified settings.
10. Check that the recipient received the fax.

17 Reprint Saved Jobs

Reprint Saved Job is a feature that allows users to store documents into folders located on the device.

Reprint Saved Job enables you to retrieve jobs which have been stored on the device using the Print Driver or CentreWare Internet Services Print Submission. Jobs are placed into a folder located on the device and can be accessed and retrieved for printing at later date. Jobs can be recalled and printed as many times as you need.

Using the Print Driver settings or CentreWare Internet Services, the job type can be set to Save Job For Reprint. When this job type is selected, an option is provided to Save Only or Save and Print. Many of the job settings are stored with the job and they can be modified at the time of printing.

All Saved Jobs are stored as encrypted files, if encryption of user data is enabled. Encryption ensures that third parties cannot read, print, scan and e-mail these files.

You can enable/disable encryption of user data, refer to User Data Encryption on page 8-1.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the device is fully functioning on the network.
- To backup jobs and folders an FTP server must be available on the network (recommended). Create an account with rights to the FTP root which the device can use to access the FTP server.

Enable Reprint Saved Jobs

1. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Reprint Saved Jobs]** link.
7. Select **[Enablement].**
8. In the **Enablement** area, select **[Enabled]** to enable Reprint Saved Jobs.
9. Click on the **[Apply]** button.

Note

All Saved Jobs are stored as encrypted files if encryption of user data is enabled. Encryption ensures that third parties cannot read, print, scan and e-mail these files. You can enable / disable encryption of user data on the **User Data Encryption** page, refer to User Data Encryption on page 8-1.

Enable Reprint Saved Jobs in your Printer Driver

Windows Operating Systems

1. At your Workstation, open the **Printers Folder**.
   - For **Windows 2000/2003** - From the **[Start]** menu, select **[Settings]** then **[Printers]**.
   - For **Windows XP** - From the **[Start]** menu, select **[Printers and Faxes]**.
   - For **Windows Vista** - From the **[Start]** menu, (select **[Control Panel]**) then select **[Printers and Faxes]**.
2. Right-click on the Xerox ColorQube 9201/9202/9203 Printer Driver.
3. Select **[Properties]**.
4. Click on the **[Configuration]** tab.
5. Click on the **[Installable Options]** button.
6. Ensure **[Installed]** is selected from the **[Job Storage]** drop down menu.
7. Click on the **[OK]** button to close the Installable Options screen.
8. Click on the **[OK]** button to close the Properties screen.

Mac Operating Systems

1. At your Mac Workstation, open the **[Printer Setup Utility]**.
2. Select the Xerox printer and click the **[Show Info]** button.
3. Click on **[Installable Options]**.
4. Select **[Installed]** from the **[Job Storage]** drop-down menu.
5. Click on the **[Apply Changes]** button.
6. Close the Printer Info box.

Manage Folders

Create New Folder

Folders and the files saved within them can be managed using CentreWare Internet Services.

1. To create a new folder, access CentreWare Internet Services. Open your web browser on your PC and enter the IP address of the ColorQube 9201/9202/9203 into the *Address (URL)* field.
2. Press **<Enter>**.
   The CentreWare Internet Services options for your device are displayed.

   Note

   To find out the IP address of your device, print a Configuration Report. Refer to How to Print a Configuration Report on page 3-2.

3. Select the **[Jobs]** options.

4. Select the **[Saved Jobs]** tab to access the folder options.
5. Select **[Create New Folder]**.
6. Input the name for the folder in the **[Name]** field.
   As a normal user you are only able to create **Public** folders. These are the other kind of folders you may see.
   - The **Public** folder has been created by a user. It can be used by any user and has no access authority limitations. Any user can access and modify the documents in this folder.
   - The **Read Only** folder is created by the System Administrator or a user as a **Read Only Public** folder. Any user can print from the folder but documents cannot be deleted or modified.
   - The **Private** folder is created by a user only when the device is in **Authentication** mode. The user marks the folder as **Private** and the folder is only visible to the Owner and the System Administrator.
7. When you have selected the appropriate Permissions, click on the **[Apply] button**.

The Folder is displayed in the **Folders List**.

Modify or Delete Folder

You can modify or delete existing folders that contain **Saved Jobs** using CentreWare Internet Services.

1. To modify a folder, access CentreWare Internet Services. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. The CentreWare Internet Services options for your device are displayed.

   Note

   To find out the IP address of your device, print a Configuration Report. Refer to Configuration Page on page 3-2.

3. Select the **[Jobs]** option.
4. Select **[Saved Jobs]** tab to access the folder options.
5. Select **[Manage Folders]**.
   The window displays all the **Public** folders and any **Private** folders belonging to you.
6. Check the box next to the folder you want to modify.
7. Select options required for the folder.
   The folder can be deleted by selecting the **[Delete Folders]** button.
   The folder and the contents of the folder are deleted from the list on this screen and the list of available folders at the device.

Saving a Job

Prior to using the Reprint Saved Jobs option, a job must be saved to a folder on the device. The folders are setup by the System Administrator using CentreWare Internet Services and can be managed by the users. Refer to Manage Folders on page 17-2 for more information.

Jobs can be saved in the folders by selecting the Save Job for Reprint Job Type when submitting a print job from your PC, or when submitting a print job using CentreWare Internet Services.

Using the Print Driver

Select or create a document on your PC.

1. Select **[Print]** from the application's **[File]** menu.
   The application Print window is displayed.
2. Select the ColorQube 9201/9202/9203 printer from the **[Printer Name]** drop-down menu.
3. Select **[Properties]** to access the print settings for the job.
4. Select the **[Job Type]** drop-down menu and select **[Saved Job...]**.
   The **Saved Job** options are displayed.
5. Program the Saved Job options as required:
   - Select **[Save]** to store the job only or **[Save and Print]** to store and print the job.
   - **Job Name** is used to enter a name for the job or select Use Document Name to use the filename of the document being submitted.
   - **Folder** is used to select a location to store the job. The **Default Public Folder** is available to all users, other folders may have restricted access.
   - **Secure Saved Job** is used to add a passcode to the job. The job can only be accessed and printed using the passcode entered here.
   - Select **[OK]** to save the settings and exit the Saved Job options.
6. Program the print features required for the saved job.

   Note

   The **Help** option provides an explanation of all the options.
7. Select **[OK]** to save the print settings.
8. Select **[OK]** on the Print dialogue window to send the job.
   The job is processed and sent to the device for saving or saving and printing, depending on the selection.

Using CentreWare Internet Services

The Print option within CentreWare Internet Services can also be used to create a Saved Job. The job file submitted must be a print ready file, such as a PDF or PostScript file.

1. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

   Note

   Click on the **[Services]** link.To find out the IP address of your device, print a Configuration Report.
2. Select **[Print]** to access the **Job Submission** options.
3. Enter the file name of the job requiring saving, or use the **[Browse]** option to locate the file.
4. Select the **[Job Type]** drop-down menu and select **[Save Job]** for Reprint.
   The Saved Job options are displayed.
   - Select **[Save]** to store the job only or **[Save and Print]** to store and print the job.
   - **Job Name** is used to enter a name for the job.
   - **Folder** is used to select a location to store the job. The **Default Public Folder** is available to all users, other folders may have restricted access.
   - **Secure Saved Job** is used to add a passcode to the job. The job can only be accessed and printed using the passcode entered here.

- Program the **Paper**, **2 Sided Printing**, **Output Colour**, **Collate**, **Orientation**, **Staple** and **Output Destination** as required.

5. Select **[Submit Job]** at the top of the page to send the job to the device over the internet.

The job is processed and sent to the device for saving or saving and printing, depending on the selection.

18 Custom Services

Validation Options

The Validation Options feature is used with the Workflow Scanning Validation Server and the Network Authentication features.

When a user enters their metadata information at the user interface, the metadata is passed to the validation server to be verified. When Validation Options is enabled, the user's ID is also passed with the validation request to the Validation Server. The user ID is recorded when the user enters their network authentication account details at the user interface.

Enable Validation Options

1. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Custom Services]** link.
7. Select **[Validation Options]** in the directory tree.
8. To have the user name sent with the validation request if the user is authenticated at the device user interface, click the **[Include User Name with validation request]** checkbox.
9. Click the **[Apply]** button.

WSD (Web Services for Devices)

Web Services for Devices specifies a lightweight subset of the overall web services protocol suite that is appropriate for network-connected devices. The Devices Profile prescribes how to use elements of core web services specifications to enable these functions:

Web Service on Devices API (WSDAPI) is an implementation of the **Devices Profile for Web Services** (DPWS) for Windows Vista and Windows Server 2008. The DPWS constrains web services specifications so clients can easily discover devices. Once a device is discovered, a client can retrieve a description of services hosted on that device and use those services.

- Send more secure messages to and from a web service.
- Dynamically discover a web service.

- Describe a web service.
- Subscribe to, and receive events from a web service.

Vista (only) operating system provides Web Services on devices as a connection protocol with printing and scanning peripherals. Web Services technology provides a common framework for describing and sharing information.

Enable WSD (Web Services for Devices)

1. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[WSD (Web Services for Devices]** in the directory tree.
7. In the **WSD Services** area, check the **[Enabled]** box to enable the services.
8. In the **WSD Services Selection** area, check individual services box you want to enable.
9. Click on the **[Apply]** button.

Xerox Standard Accounting 19

Xerox Standard Accounting (XSA) is a free feature of the device.

When enabled, XSA tracks the numbers of Copy, Print, Workflow Scanning, E-mail, Server Fax, Internet Fax and Embedded Fax jobs (when these features are installed on the device), for each user. Usage limits can also be applied to users to restrict the total numbers of copy, print, fax and scan jobs that a user can perform. Administrators can print a report which contains all XSA data.

XSA is set up through Internet Services, the device's HTTP pages displayed on your web browser. Administrators must create accounts and specify limits before users are authorized to access the device.

When XSA is set up, users must enter their account details at the device to use the device. When they have finished their job, their XSA allocation is reduced by the number of prints, copies or scans performed. When XSA is enabled, users must enter their account details in the printer driver to print documents from their workstations.

The XSA feature is mutually exclusive from any other accounting feature. If XSA is enabled at the device, you cannot enable Foreign Device Interface, Auditron or Network Accounting.

Each device supports a maximum of:

- 2500 unique XSA user IDs
- 500 General Accounts
- 500 Group Accounts.

All user IDs must be assigned to one or more group accounts.

> Note
> The XSA settings and account data are stored in the device. It is strongly recommended that you back-up the settings and data regularly using the Cloning procedure available through the Internet Services screens. Should the device lose your XSA data and settings you can restore them from the backup file that you produced by the Cloning process.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure that your device is configured on the network.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.

Enable Xerox Standard Accounting

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Accounting]** link.
5. Click on the **[Xerox Standard Accounting]** link.
6. Select **[Manage Accounting]** in the directory tree.
7. Click on the **[Enable Accounting]** button, click on the **[OK]** button when **"Properties have been successfully modified"** pop up message appears.

Continue on to the next steps to create a new group account.

Create a Group Account

8. Select **[Group Account]** in the directory tree to create a new group account.
9. In the Group Accounts area, enter an ID in the **[Account ID]** box for the new group account (for example 001). The Group Account can be numeric values up to a maximum of 12 digits. Group Account ID's must be unique.
10. Enter a name for the group account in the **[Account Name]** box (for example Xerox). The group name can be alphanumeric characters to a maximum of 32 characters. The Group Account name must be unique.
11. Click on the **[Add Account]** box, click on the **[OK]** button to confirm the account has been added. The account will appear in the Group Accounts list. Continue on to the next steps to create a new user.

Create a User Account and Set Usage Limits

Note

A group account must be created before you create user accounts.

12. Click the **[Xerox Standard Accounting]** link in the Internet Services left hand menu.
13. Click the **[Manage Accounting]** link.
14. In the **Users** area, click the **[Add New User]** button.
15. Enter an ID for the user in the **[User ID]** field. The user ID can contain alphanumeric characters to a maximum of 32 characters (for example: A10). User ID's must be unique.
16. Enter the user name (for example Jane Smith) in the **[User Name]** field. The user name can contain a maximum of alphanumeric characters. User names must be unique.

Usage Limits

17. Specify the usage limits for this account in the **[User Limits]** boxes. The maximum value for each limit is 16,000,000. Usage limits can be specified as follows:

    Black or Color Printed Impressions

    The maximum number of documents that can be printed by a user, from their workstation via the printer driver.

    Black or Color Copied Impressions

    The maximum number of copies that can be produced by a user via the Copy feature on the device.

Network Images Sent

The maximum number of documents that can be sent over the network by the user. This applies to the following features: Workflow Scanning, E-mail, Server Fax and/or Internet Fax when these features are installed on the device.

Note

If the device is set to print scan confirmation reports or Internet Fax acknowledgement reports, these documents are counted towards the user's limit.

Fax Images Sent

If Embedded Fax is installed on your device, you will see this option in Internet Services.

Fax Images Sent sets the maximum number of documents that can be faxed by a user with the Fax feature (Embedded Fax).

The device calculates the number of faxed documents by multiplying the number of images faxed (this includes cover sheets), by the number of destinations.

Embedded Fax Receive

If Embedded Fax is installed on your device, you will see this option. This sets the maximum number of documents that a user can produce from the following features on the device:

- Print Mailbox
- Poll Remote Mailbox
- Print Poll Store
- Poll Remote Fax

For example, to restrict the maximum number of prints this user can make, to *1000* prints, enter 1000 in the **[Black or Color Copied Impressions]** field. Cover sheets and banner sheets are counted as part of the job and will add to the number of impressions.

18. Click on the **[Apply]** button when you have finished setting the usage limits.

Maximum Usage Limits

The first time a user logs in to the device after they have reached their maximum usage limit, a message displays on the user interface. The message notifies the user that they have reached their limit for the feature. Users will not be able to use the feature until their limit is reset. If the user performs a copy, scan or fax job at the device, and mid way through the job their limit is exceeded, the job will continue. The device will track the number of sheets that were printed over the limit and subtract them from the user's new allocation, when it is updated by the administrator.

If the user's limit is reached before a print job is completed, an error report will print at the device to notify the user that their limit has been reached. The job will be deleted from the print queue. The job may run over due to sheets committed to the paper path.

The System Administrator has unlimited access to the device.

User limits can be reset on the Internet Services Report and Reset screen.

Using XSA at the device

When you enable XSA, users must enter a valid user name at the device to access the features.

At the Device

1. Press the **<Services>** button.
2. The **[User ID]** screen will show. Type the user ID of one of the users that you created in the Manage Accounting area of Internet Services. Use the keyboard on the screen to enter the user ID.
3. Touch the **[Enter]** button.
4. The Validation in Progress screen will show.
5. If the user is a member of more than one Group Account or General Account, they will be asked to select the account that they wish to log in to.
6. When the user is logged in, the Services screen will show. The user can now select the feature that they want to use.

Create a General Account

The XSA feature allows administrators to create both Group and General Accounts. Users must be a member of at least one Group Account. However, the creation of General Accounts is optional. General Accounts can be created to identify a subset of a group or project that a user is involved in. The XSA Report specifies the numbers of documents produced per group.

Account example

In the example below, the administrator creates a Group Account called Finance Department and two General Accounts called Company A Project and Company B Project. The administrator adds the user Jane Smith to each account.

Jane can now record any impressions that she makes at the device to a particular account.

At the device, Jane enters her user ID and selects Company A Project. The number of impressions is recorded specifically to the Company A Project.

The administrator can print an XSA Report which lists the numbers of impressions recorded for each user, Group and General Account.

1. At your Workstation, open your web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Accounting]** link.
6. Click on the **[Xerox Standard Accounting]** link.
7. Select **[General Accounts]** in the directory tree to create a new general account.
8. In the **[Account ID]** field, enter an ID for the new general account (for example 002). The General Account can be numeric values up to a maximum of 12 digits. General Account ID's must be unique.
9. Enter a name for the general account in the **[Account Name]** field (for example Xerox general). The general name can be alphanumeric characters to a maximum of 32 characters. The General Account name must be unique.
10. Click on the **[Add Account]** button. The account will appear in the General Accounts list.
11. To add a user to this account, click the **[Manage]** link in the **General Accounts** area.

12. In the **[Account]** area, make any relevant changes.
13. In the **[User Access]** area, check the boxes for the Access Right you want the General Account to have access.
14. Click on the **[Save Changes]** button. The user appears as a member of the Group and General Accounts.

Generate Report and Reset User Limits

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Accounting]** link.
6. Click on the **[Xerox Standard Accounting]** link.
7. Select **[Report and Reset]** in the directory tree.
8. To reset all usage data to 0, click on the **[Reset Usage Data]** button.
9. Click on the **[OK]** button to confirm when the **"All current usage data will be rest to zero and lost"** dialog box appears.

WARNING

The following step will delete all the XSA accounts set up for your device!

10. To delete all user, group and general accounts, click on the **[Reset to Default]** button.
11. Click on the **[OK]** button to confirm when the **"All users, accounts and usage data will be lost?"** dialog box appears.

Print a Usage Report

1. At your Workstation, open your web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Accounting]** link.
6. Click on the **[Xerox Standard Accounting]** link.
7. Select **[Report and Reset]** in the directory tree.
8. Click on the **[Generate Report]** button.
9. Right-click the **[Right-click to download]** link.
10. Select **[Save Target As]**
11. Save the **XSA Report.csv** file to your desktop.

Enable XSA in your Windows Print Driver

1. From the **[Start]** menu select **[Printers and Faxes]** (Windows XP), or select **[Settings]** and then **[Printers]** (Windows 2000/20003).
2. Right-click on the printer driver.
3. Select **[Properties]**.
4. Select **[Configuration]**.

5. Select **[Accounting]**.
6. From the **Accounting System** drop-down menu, select **[Xerox Standard Accounting]**.
7. Select **[Prompt for Every Job]** if you want users to enter their User and Account ID each time they print.
8. You may also select the **[Mask User ID]** and **[Mask Account ID]** checkboxes to show asterisks (******) when ID's are entered.
9. Select the **[Save Accounting Codes]** to save selection.
10. Otherwise select **[Use Default Accounting Codes]** and enter the default user ID and the default Account Type.
11. Enter the default Account ID.
12. Click **[OK]**.
13. Click **[OK]** to exit.

When you use the printer driver to print a document you will be asked to enter your user ID.

Enable XSA in your Apple Macintosh Print Driver

Mac OS X

1. Open a document to print and select **[File]** and then **[Print]**.
2. From the Print Options Menu select **[Printer Features]**.
3. Select the **[Feature Sets]** menu.
4. Select **[JCL]**.
5. Select **[Accounting]** to enable it.
6. Print the document.

Back-up XSA Data and Settings and Clone to Another Xerox Device

The Cloning feature enables you to copy settings, including XSA settings and account information, to a file on your workstation or Server. You can then use this file to restore the data and settings on the same device or to clone other devices. You can only clone XSA settings to another Xerox device that supports the XSA feature.

Check that the device you want to clone settings to supports XSA

1. At a networked workstation, open the web browser and enter the *IP address* of the device that you want to clone to in the Address bar, and press **[Enter]**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Cloning]** in the directory tree.
7. From the display of available check boxes, verify that Accounting is among them.
8. Click again on the **[General Setup]** link, then select **[Configuration]** in the directory tree, and verify that both devices have the same System Software Version.

To make a Back-up file

1. At your workstation, open the web browser and enter the *IP address* of the device with the settings that you want to copy, in the Address bar, and press **[Enter]**.

2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Cloning]** in the directory tree.
7. From the display of available groups, select the settings that you wish to clone. To clone all features, click on the **[Clone]** button, or to customize the configuration file disable any of the features by clicking the checkboxes next to the feature(s) and then click on the **[Clone]** button.
8. Right-click on the **[.dlm]** link that appears and select **[Save Target As]**.
9. A dialog box will prompt you to specify and name and location for the cloned file. Ensure the extension reads **.dlm**.
10. Click on the **[Save]** button. The.dlm file can now be used to restore the information to the same device or to clone other devices.

To Restore Settings or Clone Settings to Another Device

Note

This procedure will cause the device to reboot and will be unavailable over the network for several minutes.

1. Open your web browser and enter the *IP address* of the device that you wish to restore or clone the settings to. Press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Select **[Cloning]** in the directory tree.
7. In the **[Install Clone File]** area, click on the **[Browse]** button.
8. Locate the **[.dlm]** clone file.
9. Click on the **[Install]** button.

   The device will be unavailable over the network for several minutes. Once rebooted a Configuration Report will print, if enabled.
10. The XSA settings and data will be restored as they were when the back-up file was created. If you are cloning another device you may want to change, delete or reset the XSA accounts as appropriate for the new device.

20 Network Accounting

Network Accounting provides the ability to manage usage of the device with detailed cost analysis capabilities. Print, Scan, Fax, and Copy jobs are tracked at the device and stored in a job log. Jobs require an authentication of User ID and Account ID and this information is logged with the job details in the job log.

The device requires the Network Accounting Kit to be installed and network access to a Xerox certified Network Accounting third party software solution. Refer to your Xerox Sales Representative for further information.

CentreWare Print and Fax Drivers are required to be installed on workstations. The user is prompted for accounting information when submitting jobs to the device.

The job log information can be compiled at the accounting server and formatted into reports.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the device is fully functioning on the network prior to installation.
- Locate the Network Accounting Kit.
- Ensure that the TCP/IP and HTTP protocols are configured on the device as per Enable TCP/IP and HTTP at the Device on page 2-5.

  This is required to access CentreWare Internet Services to configure Network Accounting.
- Install and configure the Xerox certified network accounting solution package on your network. Refer to the manufacturer's instructions with the network accounting package to complete this task.
- Test communication between the accounting server and the device. To do this:

  Go to your network accounting server and open a web browser. Enter the *IP Address* of the device in the address bar, and press **[Enter]**. The device's Internet Services web page will appear.

  If you do not have a web browser, test connectivity by pinging the IP address of the device from your network accounting server.

Enable and Configure Network Accounting

When you purchased the Network Accounting Kit, you received the information and SIM required to install this feature. Following the supplied instructions for full details, with the device powered on, the SIM is inserted into an orange slot on the device's backplane. An Options Assist screen pops up to help with installation.

To Enable the Network Accounting feature at the Device

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Accounting Settings]**.
5. Touch **[Accounting Mode]**.
6. Touch **[Network Accounting]** and touch **[Save]**.

Configure Network Accounting

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Accounting Settings]**.
5. Touch **[Accounting Mode]**.
6. Touch the **[Network Accounting]** button to enable it, a **Network Accounting Configuration** menu will display on the right hand side of the touch screen.
7. Touch the **[Customize Prompt]**, select the required option from the **[Display Prompt 1 Only]** drop down menu.
8. Touch **[Prompt 1 Label]**, and enter an ID between 1 and 32 characters and touch **[Save]**.
9. Touch **[Prompt 2 Default Value]**, and enter an ID between 1 and 32 characters and touch **[Save]**.
10. Touch the **[Mask Entries]** box to place a tick, and touch **[Save]** to return to the **Accounting Mode** screen.
11. Touch **[Code Entry Validation]**.
12. Touch the **[Enabled]** button to enable authentication or **[Disabled]** to disable authentication.
    - **Authentication Enabled**
      If you want to track copy, print and scan usage by both User ID, Account ID and amount of resources each user account uses (for example, types and sizes of paper stock, duplex or simplex, stapled or not stapled) ensure that Authentication is Enabled. Users will then be required to enter a valid User ID and an Account ID for any job. The User ID and Account ID are alphanumeric strings between 1 and 32 characters in length.
    - **Authentication Disabled**
      Disabling Authentication allows the device to accept both valid and invalid User and Account ID's. Authentication Disabled is useful if conducting an analysis for the resources used on a particular device before Authentication controls are instituted. Users will still be required to enter at least one character into the User and Account ID fields.
13. Touch the **[Save]** button to retain the settings.
14. Touch the **[Save]** button.
15. Touch the **[Log In / Out]** button, and touch **[Logout]** to log out.
16. To verify Accounting is enabled, press the **[Services]** button on the front panel.
17. The Touch Panel should display a screen with two buttons. One is the **[User ID]** button and the other is the **[Account ID]** button. This indicates the system has enabled accounting successfully.
18. Go to the Network Accounting Server to Activate the Device
    Open the Network Accounting application and configure it so that the IP Address (or fully qualified domain name) of device is entered as the destination for retrieval of data. Refer to the manufacturer's documentation with your Network Accounting server to complete this task.

Enable Network Accounting in your Windows Print Driver

Windows 2000

1. From the **[Start]** menu select **[Printers and Faxes]**.
2. Right-click on the device printer icon.
3. Select **[Properties]**.
4. Select **[Configuration]**.
5. Select **[Accounting]**.
6. Select **[Xerox Network Accounting]** from the **Accounting System** drop-down menu.
7. Select **[Prompt for Every Job]** if you want users to enter their User and Account ID each time they print.
8. You may also select the **[Mask User ID]** and **[Mask Account ID]** checkboxes to have the asterisk (***) character echoed when this information is entered.
9. Otherwise select **[Use Default Accounting Codes]** and enter the **Default User ID** and the **Default Account ID**.
10. Click **[OK]**.
11. Click **[OK]** to exit.

Windows XP, Vista

1. From the **[Start]** menu select **[Settings]** and then **[Printers]**.
2. Right-click on the device printer icon.
3. Select **[Properties]**.
4. Select the **[Configuration]** tab.
5. Check the **[Enable Accounting]** box.
6. Select **[Prompt for Every Job]** if you want users to enter their User and Account ID each time they print.
7. You may also select the **[Mask User ID]** and **[Mask Account ID]** checkboxes to have the asterisk (***) character echoed when this information is entered.
8. Otherwise select **[Use Default Accounting Codes]** and enter the default user ID and the default account ID.
9. Click **[OK]**.
10. Click **[OK]** to exit.

Enable Network Accounting in your Mac Print Driver

Mac OS X

1. Open a document to print and select **[File]** and then **[Print]**.
2. Select the Xerox printer.
3. From the **Copies and Pages** menu select **[Accounting]**.
4. Select **[Xerox Network Accounting]** from the **Accounting System** menu.
5. Select **[Prompt for Every Job]** if you want to enter your Network Accounting User and Account ID when you print.
6. You may also select the **[Mask User ID]** and **[Mask Account ID]** checkboxes to hide the user and account ID information.
7. Otherwise select **[Use Default Accounting Codes]** and enter a default user ID and a default account ID.
8. To save your settings select the **[Presets]** menu and click **[Save As]**.

9. Enter a name to define the preset, for example: *Accounting*.
10. Click **[OK]**. Ensure the *Accounting* preset is selected in the **Presets** menu each time you print.
11. Click **[Print]**.
12. Enter your Network Accounting information.
13. Click **[OK]** to print the document.

Test Network Accounting

1. Open an application and print a job. Verify that you are presented with the User ID and Accounting ID screen.
2. Enter a valid User and Accounting ID and click **[OK]** (If you selected **[Save Accounting Codes]** it will only be necessary to enter this information the first time the driver is used).
3. If your print job does not print, try to copy a job at the device using the same Account and User ID. If the copy job completes then the Account and User ID are valid.
4. It may be necessary to check the network accounting solution software or server configuration to verify the User ID and Account ID.
5. Distribute the printer drivers with the Network Accounting option already selected (if possible). If the printer drivers are distributed without the option enabled, workstation users will need to configure the drivers. If the drivers are not properly configured, jobs sent to the device will be deleted.

21 Xerox Secure Access

Administrators can configure the device so that users must be authenticated and authorized before they can access specific services or areas. Xerox Secure Access provides a means of authenticating users via an authentication server and optional card reader.

This convenient security solution allows people to simply swipe the ID card at the device to unlock access to features that can be tracked for accounting and regulatory requirements.

Secure Access and Accounting

Secure Access can be enabled with the **Network Accounting**, **Xerox Standard Accounting** and **Workflow Scanning** features to provide accounting functionality.

Note

Secure Access cannot be enabled at the same time as Foreign Device Interface.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the Xerox device is fully functional on the network. TCP/IP and HTTP protocols must be configured so that Internet Services can be accessed.
- Ensure the Xerox Secure Access authentication server is installed and configured with user accounts. Refer to the documentation with the authentication server to complete this task.

  Contact your Xerox Sales Representative if you do not have the Xerox Secure Access authentication server.

  Note

  There must be a mapping between the accounts created on the authentication server and accounts created in the Local User Information Database or remote Authentication server (see steps 4 and 5).

- Connect and configure your card reader, if required. Attach the card reader to the left hand shelf on the device. Place the controller box on the floor at the back of the device.
- Ensure that SSL (Secure Sockets Layer) is configured on the Xerox device via Internet Services.
- To configure Authorization locally, the Local User Information Database must be configured. For instructions, refer to the Local User Information Database section within the System Administration CD1. There must be a mapping between the accounts created on the Authentication Server and the

Local User Information Database (the user names must match so that the device can cross reference each user as they log in at the device).

- To configure Remote Authorization, the LDAP server must be configured on the device and Authorization Access configured. For instructions, refer to the LDAP section within the System Administration CD1. There must be a mapping between the accounts created on the Authentication Server and the LDAP server (the user names must match so that the device can cross reference each user as they log in at the device).

Access Authentication Configuration

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.

The first time you access the Authentication Configuration screen you will be asked to change the System Administrator Password.

The System Administrator password is used to access Tools at the device user interface, and change settings via Internet Services.

If you do not see the Device System Administrator Password screen, go to the **Configure Authentication** instructions, below.

8. Enter a new password in the **[New Password]** and **[Retype New Password]** areas.

   IMPORTANT: Do not forget the password or you could be completely locked out of the system, requiring a service call.

   Note

   The default User Name cannot be changed.

9. Click **[Next]**.

Configure Authentication

10. On the Authentication Configuration page, from the **Device User Interface Authentication** drop-down menu select **[Xerox Secure Access]**.
11. Select your required option from the **Web User Interface Authentication** drop-down menu. When a user attempts to access Internet Services they are prompted to enter their login information. The option selected from the web user interface Authentication menu defines how the device will validate the user's rights to access Internet Services. This is required because if the user normally authenticates at the device with a card reader, there would be no method for the device to authenticate users who access Internet Services from their workstations.
    - Select **[Locally on the Device]** to validate users listed in the Local User Information Database. This option requires you to configure accounts in the Local User Information Database.
    - Select **[Remotely on the Network]** to validate users via an Authentication Server. This option requires you to have a server that will provide authentication of user login details. Authentication via Kerberos (Solaris, Windows 2000/2003), SMB (Windows NT4/2000) or LDAP is supported.

- Select **[Xerox Secure Access]** to allow users to be authenticated and authorized before they can access specific services or areas. Xerox Secure Access provides a means of authenticating users via an authentication server and optional card reader.
- Select **[CAC/PIV]** (Common Access Card/Personal Identity Verification) solution brings an advanced level of security to sensitive information. Organizations can restrict access to the walk-up features of a Xerox device. This ensures only authorized users are able to copy, scan, e-mail and fax information. The key benefit of this solution is its two-factor identification requirement. Users must insert their access card and enter a unique Personal Identification Number (PIN) at the device. This provides added security in the event that a card is lost or stolen. Once validated, a user is logged into the Xerox device for all walk-up features. The system allows for functions to be tracked for an added layer of security.

12. Select the Authorization method in the **Authorization** drop-down menu. The card reader and Authentication Solution authenticates (validates) the user. The Authorization method determines which areas of the device a user is allowed to access.
    There are two options:
    - Select **[Locally on the Device]**: if you want the device to check the Local User Information Database for levels of authorization.
    - Select **[Remotely on the Network]**: if you want to use networked databases such as LDAP server to determine levels of authorization.

Personalisation

13. Click **[Automatically retrieve user's e-mail address from LDAP]** if required.
14. Click on **[Next]**.

Configure Xerox Secure Access on the Device

Before you complete these steps ensure that the Xerox Secure Access authentication server has been configured to point to the device.

15. At the **Authentication Configuration** screen, in the **Authentication** area, click the **[Configure]** button next to **Device User Interface Authentication** Xerox Secure Access.
16. If the Authentication Solution has been configured correctly the address information should be populated with the address of the Authentication Solution server. If the information is incomplete or incorrect, click on the **[Manually Configure]** button.
17. In the **Server Communication** area, select either **[IPv4 Address]** or **[Hostname],** and enter the IP Address and Port or Host Name and Port details.
18. Enter the details in the **Path** box.

    Note

    Enter the HTTP path of **[public/dce/xeroxvalidation/convauth]** and port number of **[1824]** to facilitate communication.

19. If you are using the Network Accounting feature, the Xerox device can be set to automatically obtain accounting data for the user from the Authentication server when the user authenticates. This reduces the number of screens that the user is presented with when they login at the device.

To implement this feature, select **[Automatically apply Accounting Codes from the server]**.

If you want the user to provide accounting data manually at the user interface, select **[User must manually enter accounting codes at the device]**.

20. If you require users to use a Xerox Secure Access device to log in (for example, a card reader), select **[Restricted access via Xerox Secure Access Device]**. If you want to allow users to enter their login details on the screen keyboard select **[Enable alternate access via on-screen keyboard]**.
21. In the **Device Instructional Blocking Window** area, enter text in the **[Window Title]** field to define a title that will display on the Xerox device screen.
22. Enter text in the **[Instructional Text]** field to define a prompt that will show on the Xerox device screen to tell the user what they need to do to be authenticated at the device.

    Note

    If the Title and Prompt have been configured on the Xerox Partner authentication server, then this information will override the Default Title and Prompt text entered within Internet Services.

23. Click **[Save]**.
24. Click the **[Configure]** button next to **Web User Interface Authentication**.
25. Verify the information configured for the web user interface authentication. If you have selected **Remotely on the Network**, enter the address of the authentication server that will validate user accounts.
26. Click **[Save]** or **[Close]**.

Authorization Configuration

27. If you selected **Locally on the Device** for the method of Authorization, click **[View]** next to Local User Information Database. Verify the information is correct.

    If you selected **Remotely on the Network** for the method of Authorization, click **[Configure]** next to LDAP Server and verify the information is correctly configured. At the LDAP screen, click **[Authorization Access]** and enter the group names from your LDAP server that you want to grant access to. For more information, refer to **LDAP Configuration** in this guide.
28. Click **[Save]** or **[Close]**.

Personalization

29. If you selected 'Automatically retrieve user's e-mail address', click **[Configure]** next to LDAP Server and verify the information is correctly configured.

    Note

    If you have already checked the LDAP server information, this step is optional.

30. Click **[Save]** button to save the settings and return to the **Authentication Configuration** page.

Device Default State Configuration - Set Authentication to control access to individual Services

31. In the **Device Default State Configuration** area, click on the **[View]** button for **Service Registration**.
32. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
33. Click on the **[Save]** button and return to the **Authentication Configuration** page.

Set Authentication to control access to individual Features

34. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
35. In the **Tools & Feature Access** page, under **Presets**, select either:
    - **Standard Access - Only Lock Tools**
    - **Open Access - Unlock All Tools and Features**
    - **Custom Access**

If you select **[Custom Access]**, for each feature you can either select **[Unlocked]** or **[Locked]** from the drop down menu.

36. Click on the **[Apply]** button.
37. Click on the **[OK]** button when you see the window that says **"Properties have been successfully modified"**.
38. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Use Secure Access

At the Device

1. Touch/press an area of the device that you have locked.
2. Read the user interface prompt to determine what you need to do to be authenticated at the device. Authentication methods include:
   - Swipe a card
   - Place a proximity card near to the reader
   - Enter a user ID or PIN number.

If you need to enter information, touch the **[Keyboard Access]** button and enter your login information.

3. The screen may request further information, such as a primary PIN or password, or account information. The primary PIN may have been set on the Xerox Secure Access authentication server. The account information may be requested because an accounting option is configured on the device.
4. The Xerox device will confirm successful authentication and you will now have access to the features.
5. When you have finished using the features, press the **[Clear All]** button on the keypad to close your account.

22 Software Upgrade

The Software Upgrade feature allows the customer to upgrade the device software as requested by a Xerox Customer Support Center Representative, without needing a Customer Service Representative to be present.

When Should I Upgrade the Software?

Xerox is continually seeking to improve its products and a software revision may become available to improve functionality on the device. Your Customer Support Center Representative will instruct you to upgrade your device when it is necessary.

How Do I Upgrade the Software?

IMPORTANT: Any jobs in the queue must be allowed to complete or be deleted before initiating a software upgrade.

There are two methods for upgrading the software on the device:

- Over a network connection using Internet Services via a web browser.
- Auto upgrade.

1. Software Upgrade via Network Connection

If your device is connected to the network it is possible to upgrade the software through Internet Services. The device will need to be configured for TCP/IP and HTTP.

2. Auto Upgrade

If performing a software upgrade on the device via Internet Services it is possible to set the Auto Upgrade feature to schedule automatic device software upgrades from a central server at a specific time on a regular basis.

To determine whether your device has a network connection, print a Configuration Report as follows:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**

Upgrade via Internet Services

Note

This procedure will delete any current jobs in the device print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software.
All configured network settings and installed options will be retained by the device after the Software Upgrade process.

Information Checklist

Before starting the installation procedure, please ensure the following items is available or has been performed:

- Obtain the new software upgrade file for your device from the www.xerox.com website or from your Xerox Customer Support Representative.

  The upgrade file will have an extension of .dlm (dynamically loaded module). Download the upgrade file to a local or network drive. You will be able to delete the file after the upgrade procedure.

It is important to obtain the correct upgrade file for your particular model of device.

System Software Version

To determine which model of device you have, check the system software version.

At the Device

1. Press the **[Machine Status]** button.
2. View the **Software Version**.

Note

TCP/IP and HTTP protocols must be enabled on the device so that the device can be accessed via the web browser.

Procedure

1. At your Workstation, open the web browser and enter the *IP Address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Click on the **[Upgrades]** in the directory tree.
8. Check to enable **[Upgrades]** box.
9. Click on the **[Apply]** button.
10. Click on the **[Manual Upgrade]** in the directory tree.
11. In the **Manual Upgrade** area, click on **[Browse]** to locate the software upgrade file **[.dlm]** obtained earlier.

12. Click on the **[.dlm]** file obtained earlier.
13. Click on the **[Open]** button.
14. Click on the **[Install Software]** button to proceed with the upgrade.
    - If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
    - Click on the **[Login]** button.
15. The file will be sent to the printer and will disable the printing functionality. The web browser will become inactive and you will not be able to access the device via this method until the upgrade has completed and the device has rebooted. The upgrade should take no longer than 30 minutes.
16. Once the device has completed the upgrade it will reboot automatically. The Configuration Report will print (if enabled). Check the Configuration Report to verify that the software level has changed.

Auto Upgrade

You can set the device to automatically schedule device software upgrades from a central server at a specific time on a regular basis.

> Note
> This procedure will delete any current jobs in the device print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software.
> All configured network settings and installed options will be retained by the device after the Software Upgrade process.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Obtain the new software for your device (this will have an extension of .dlm (dynamically loaded module) from the www.xerox.com website or from your Xerox Customer Support Representative.
- Download the upgrade file to a local or network drive. You will be able to delete the file after the upgrade procedure.
- TCP/IP and HTTP protocols must be enabled on the device so that the device web browser can be accessed.

At your Workstation,

1. Open the web browser and enter the *IP Address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Click on the **[Upgrades]** in the directory tree.
8. Check to enable **[Upgrades]** box.
9. Click on the **[Apply]** button.

Set the Auto Upgrade Time

10. Click on the **[Auto Upgrade]** in the directory tree.
11. Check the **[Enabled]** box to enable the **Schedule Upgrade** feature.
12. Select either **[Hourly]** or **[Daily]** to activate the feature accordingly, in the Refresh Start Time section.
13. If **[Daily]** has been selected, enter the required time for the upgrade to be performed.
14. For **[Protocol]**, select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
15. Enter the IP Address and Port or the Host Name and Port of the server where the software upgrade file (obtained earlier) is located.
16. Enter the path to the upgrade file on the server in the **[Directory Path]** field.
17. Enter the **[Login Name]** and **[Password]** for the server.
18. Click on the **[Apply]** button to accept the changes.

The upgrade will now be performed automatically on the device at the time specified. Once the upgrade process starts network connectivity with the device will be unavailable, including access from Internet Services. The upgrade progress can be monitored from the device screen interface.

Note

Software Installation will begin several minutes after the software file has been submitted to the device. Once Installation has begun all Internet Services from this device will be lost, including this web user interface. The installation progress can be monitored from the local user interface.

23 Server Fax

The Server Fax feature enables users to send documents to one or more fax devices via the telephone network without having a dedicated telephone line connected to the device. This is achieved by providing a network 'fax server' with its own links to the telephone system. The device requires the Internet/Server Fax Kit to be installed and a network connection to a Xerox certified third party server fax solution to enable Server Fax. Refer to your Xerox Sales Representative for further information.

This section contains instructions to configure a fax filing location (repository) on your server. The fax server retrieves the documents from the filing location and transmits them via the telephone network. The fax server manages the fax transfer and has the ability to send confirmation reports which are printed at the device.

Server Fax and Embedded Fax

The Embedded Fax and Server Fax services are mutually exclusive and only one of them can be enabled at any time. If Server Fax is currently enabled and Embedded Fax is then enabled, Server Fax will be disabled automatically. If Embedded Fax is currently enabled and Server Fax is then enabled, Embedded Fax will be disabled automatically.

Server Fax Authentication and Authorization

Authentication (Service Access Control) can be enabled on the device to prevent unauthorized access to the network options. If Authentication is enabled a user will be prompted to enter a user name and password, or a PIN, before they can access the Fax feature. For a full description of the Authentication feature refer to the Authentication section in this guide. Authentication can be configured after Server Fax has been installed.

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure the device is fully functioning on the network prior to enabling Server Fax.
- Install the Scanning Hardware Kit.

  Refer to the instructions contained with the kit to complete this task. Contact your Xerox Sales Representative if you do not have the Scanning Hardware Kit.
- Locate the Internet/Server Fax Subscriber Installation Module (SIM).

  To install Server Fax on the device, you will need the Internet/Server Fax SIM. Following the supplied instructions for full details, with the device powered on, the SIM is inserted into an orange slot on the

device's backplane. An Options Assist screen pops up to assist with installation. Contact your Xerox Sales Representative if you do not have the plastic SIM.

- Ensure that the TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 2-5.

  This is required to access the device's Internet Services web pages, which can be used to configure E-mail settings from a network connected workstation's web browser.

  For instructions on how to configure TCP/IP and HTTP, refer to Configure Protocols with Internet Services on page 2-9.
- Install and configure the Xerox certified fax server solution on your network. Refer to the manufacturer's documentation contained with the server fax solution for instructions to complete this task.
- If the server fax solution uses the TCP/IP protocol to communicate, it is recommended that the server be assigned a static IP address. However, dynamic IP Addressing may be used provided DNS settings are fully configured and the DHCP server has been configured with sufficient lease time so that the normal maintenance and service down times of the fax server does not result in a change in IP address.

Enable Server Fax

Server Fax is an optional feature for the device. When you purchase the Internet/Server Fax Kit you will receive the information and hardware required to install this feature. The Kit contains the Subscriber Installation Module (SIM), and self explanatory instructions, used to install the Server Fax option. In addition, before installing the Server Fax feature, make sure that the Workflow Scanning/E-mail Kit was installed.

Print a Configuration Report to verify that Server Fax is an Installed Option.

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

Configure a Server Fax Filing Location (Repository)

Once configured, the device will transfer images that a user has specified to be faxed, to a directory known as the fax repository on the fax server. The fax server monitors the fax repository for documents to be faxed.

Select your required transfer method from the list below.

- **FTP (File Transfer Protocol):** Requires an FTP server running on a server or a workstation.
- **SMB (Server Message Block):** Available for filing to an environment that supports the SMB protocol.
- **HTTP/HTTPS:** Supports scans to a web server using a CGI script.
- **SMTP (**Simple Mail Transfer Protocol): Available to file to a mail server.

Configure a Fax Repository using FTP

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed:

- Ensure that File Transfer Protocol (FTP) services is running on the server or workstation where images to be faxed by the device will be stored. Note the IP address or host name.
- Create a user account and password for the device. When the Server Fax feature is used, the device logs in using the account, transfers the file to the server or workstation and logs out. Note the user account and password details.
- Create a directory within the FTP root to be used as a fax repository. Note the directory path.

Test the FTP connection by logging in to the fax repository from a PC with the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function check the user account access rights and the FTP service setup.

Enter the Fax Repository Details via Internet Services

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. Select FTP from the **[Protocol]** drop down menu.
9. Select either **[IP Address]** or **[Host Name]**.
10. Enter the IP Address and Port or Host Name and Port of the FTP location.
11. Type in the path to the location of the fax repository in **[Document Path]**. Enter the full path to the directory, starting at the root of FTP services. For example: */(directory name)/(directory name)*.
12. In the **[Login Credentials to Access the Destination]** area, select either **[Authenticated User]** or **[System]**, enter the user account and password in the **[Login Name]** and **[Password]** entry boxes. Select **System** to have the system log into the server, or **Authenticated User** to have your Authentication Server determine access.
13. Click on the **[Apply]** button to accept the changes.

Configure General Settings

1. Select **[Defaults]** in the directory tree.
2. To print a Confirmation Sheet after every Server Fax job, click on the **[Edit]** button in the **General** section, then select **[On]** from the drop down menu. The Confirmation Sheet specifies the success or failure of the Server Fax job. If the fax is successful the location of the document on the fax server is also specified.
3. Check the **[User Name]** and **[Domain]** boxes if you want these to appear on the Job Log. The Job Log is filed in the fax repository with the fax job.
4. Click on the **[Apply]** button, to accept changes and return to the **Server Fax: Defaults** screen.
5. Other settings such as:
   - **Server Fax:** has the following setting that can be adjusted; 2-Sided Scanning, Content Type, How Original was Produced and Resolution.
   - **Image Quality:** has the following setting that can be adjusted; Lighten/Darken and Suppression.

- **Layout Adjustment:** has the following setting that can be adjusted; Original Orientation and Original Size.
- **Filing Options:** has the following setting that can be adjusted; Delay Start.

6. To change any feature settings, within each setting area click on the **[Edit]** button, select the feature to be changed and click on the **[Save]** button to return to the **Server Fax: Defaults** screen.

At the Device

1. Press the <Services> button.
2. Touch the **[Server Fax]** icon.
3. Enter a valid fax number, touch **[Add]**.
4. Load a document in the document handler and press the **[Start]** button.
5. Verify that your fax is received at the specified fax device.

Configure a Fax Repository using SMB

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Create a shared folder to be used as a fax repository. Note the Share Name of the folder and the Computer Name or Server Name.
- Create a user account and password for the device with full access rights to the fax repository. Note the user account and password.
- Test the settings by attempting to connect to the shared folder from another PC by logging in with the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function check the user account access rights.

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. Select **[SMB]** from the **Protocol** drop down menu.
9. Select **[IP Address]** or **[Host Name]** and enter either IP address and Port number or Host Name and Port number of the computer where the fax filing repository (SMB server/workstation) is located.
10. Enter the **[Port Number]** if required (it is recommended to retain the default setting).
11. Enter the Share Name in **[Share]**.
12. Enter the Document Path (as it relates to the share) where the fax repository is located, in **[Document Path]**. For example: If the path is *sharename\wc\fax, enter \wc\fax* in **[Document Path]**.
13. In the **[Login Credentials to Access the Destination]** area, select either **[Authenticated User]** or **[System]**, enter the user account and password in the **[Login Name]** and **[Password]** entry boxes. Select System to have the system log into the server, or Authenticated User to have your Authentication Server determine access.

14. Click on the **[Apply]** button to accept the changes.

Configure General Settings

1. Select **[Default]** in the directory tree.
2. To print a Confirmation Sheet after every Server Fax job, click on the **[Edit]** button in the **General** section, then select **[On]** from the drop down menu. The Confirmation Sheet specifies the success or failure of the Server Fax job. If the fax is successful the location of the document on the fax server is also specified.
3. Check the **[User Name]** and **[Domain]** boxes if you want these to appear on the Job Log. The Job Log is filed in the fax repository with the fax job.
4. Click on the **[Apply]** button to accept changes.
5. Other settings such as:
   - **Server Fax:** has the following setting that can be adjusted; 2-Sided Scanning, Content Type, How Original was Produced and Resolution.
   - **Image Quality:** has the following setting that can be adjusted; Lighten/Darken and Suppression.
   - **Layout Adjustment:** has the following setting that can be adjusted; Original Orientation and Original Size.
   - **Filing Options:** has the following setting that can be adjusted; Delay Start.
6. To change any feature settings, within each setting area click on the **[Edit]** button, select the feature to be changed and click on the **[Save]** button toreturn to the **Server Fax: Defaults** screen.

At the Device

7. Select the **[Fax]** button from the touch screen, then touch **[OK]**.
8. Enter a valid fax number. Press **[Add]**, then **[Close]**.
9. Load a document in the document handler and press the green start button.
10. Verify that your fax is received at the specified fax device.

Configure a Fax Repository using HTTP/HTTPS

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- Ensure that web services are installed on the server where you want to store scanned images. Examples of web servers include: Microsoft Internet Information Services (IIS) and Apache. Note the IP address or host name of the server.
- For HTTPS, ensure that your web server is installed with a secure certificate.
- Create a user account and password for the device. When a document is scanned, the device logs in using the account, transfers the file to the server or workstation and logs out. Note the user account and password details.
- Create a directory on the HTTP/HTTPS server to be used as a scan filing location (repository). Note the directory path.
- Note any script that is required to be run.

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. Select **[HTTP]** or **[HTTPS]** from the **[Protocol]** drop down menu.
9. Select **[IP Address]** or **[Host Name]** and enter IP Address and Port or Host Name and Port of the computer where the fax filing repository (HTTP or HTTPS server) is located.
10. Enter the **[Script Path]** and file name (from HTTP root). Click on the **[Get Example Scripts]** link for further information.
11. Enter the path to the scan repository in the **[Document Path]** box.
12. Enter the **[Login Name]** and **[Password]** for the fax repository. Also, select **[System]** to have the system log into the server, or **[Authenticated User]** to have your Authentication Server determine access.
13. Click on the **[Apply]** button to accept the changes.

Configure General Settings

1. Click **[Defaults]** in the directory tree.
2. To print a Confirmation Sheet after every Server Fax job, click on the **[Edit]** button in the **General** section, then select **[On]** from the drop down menu. The Confirmation Sheet specifies the success or failure of the Server Fax job. If the fax is successful the location of the document on the fax server is also specified.
3. Check the **[User Name]** and **[Domain]** boxes if you want these to appear on the Job Log. The Job Log is filed in the fax repository with the fax job, click on the **[Save]** button to accept changes and return to the Default page
4. In the **Server Fax** section, click on the **[Edit]** button, select the desired options for 2-Sided Scanning, Content Type, How Originals was Produced and Resolution, click on the **[Apply]** button to accept changes and return to the Default page.
5. In the **Image Quality** section, click on the **[Edit]** button to Lighten or Darken the document, and select the Suppression option, click on the **[Apply]** button to accept changes and return to the Default page.
6. In the **Layout Adjustment** section, click on the **[Edit]** button, select the desired option for Original Orientation and Original Size, click on the **[Apply]** button to accept changes and return to the Default page.
7. In the **Filing Options** section, click on the **[Edit]** button to set the default for Delay Start, click on the **[Apply]** button to accept changes and return to the Default page.

At the Device

1. Touch the **[Fax]** button from the touch screen, then touch **[OK]**.
2. Enter a valid fax number. Touch **[Add]**, then **[Close]**.
3. Load a document in the document handler and press the **[Start]** button.
4. Verify that your fax is received at the specified fax device.

Configure a Fax Repository using SMTP

Information Checklist

Before starting the installation procedure, please ensure the following item is available or has been performed.

- Obtain the domain name of your SMTP mail server.

At your Workstation

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Services]** link.
6. Click on the **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. Select **[SMTP]** from the **Protocol** drop down menu.
9. Enter details in the **[Domain]** field.
10. Click on the **[Apply]** button to accept the changes.

Configure General Settings

1. Select **[Default]** in the directory tree.
2. To print a Confirmation Sheet after every Server Fax job, click on the **[Edit]** button in the **General** section, then select **[On]** from the drop down menu. The Confirmation Sheet specifies the success or failure of the Server Fax job. If the fax is successful the location of the document on the fax server is also specified.
3. Check the **[User Name]** and **[Domain]** boxes if you want these to appear on the Job Log. The Job Log is filed in the fax repository with the fax job.
4. Click on the **[Apply]** button to accept changes.
5. Other settings such as:
   - **Server Fax:** has the following setting that can be adjusted; 2-Sided Scanning, Content Type, How Original was Produced and Resolution.
   - **Image Quality:** has the following setting that can be adjusted; Lighten/Darken and Suppression.
   - **Layout Adjustment:** has the following setting that can be adjusted; Original Orientation and Original Size.
   - **Filing Options:** has the following setting that can be adjusted; Delay Start.
6. To change any feature settings, within each setting area click on the **[Edit]** button, select the feature to be changed and click on the **[Save]** button to return to the **Server Fax: Defaults** screen.

At the Device

7. Select the **[Fax]** button from the touch screen, then touch **[OK]**.
8. Enter a valid fax number. Press **[Add]**, then **[Close]**.
9. Load a document in the document handler and press the green start button.
10. Verify that your fax is received at the specified fax device.

24 Troubleshooting

Troubleshooting: Workflow Scanning

If you are experiencing problems with Workflow Scanning, first verify that the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test print from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Is the device functioning on the network as a printer?

Configure your device on the network or resolve any networking issues before attempting to use the Workflow Scanning feature. For instructions to configure the device on the network see Enable TCP/IP and HTTP at the Device on page 2-5.

Ensure Workflow Scanning is installed properly on the device.

At the device, verify that you have a Workflow Scanning button on the device screen interface and that this is not grayed out or unavailable.

It may be necessary to press the Services button to view the Workflow Scanning button on screen.

Is the Workflow Scanning Button Available on the Device?

If there is no Workflow Scanning button available on the device, install the Scanning Kit and configure the Workflow Scanning feature. For instructions, refer to Workflow Scanning on page 10-1.

> Note
>
> If you have installed Workflow Scanning but the button is grayed out or unavailable, at the device press the Log In / Out button. Enter the Administrator's User Name (default is **[1111]**), touch **[Next]**, enter Password (default is **[1111]**), touch **[Enter]**, touch the Tools tab, and touch User Interface Settings. Touch Service Enablements, then Workflow Scanning, set the service to Enable, and touch Save. Reboot the device with the Power On/Off button. For instructions on use of the Power On/Off button, click the Previous Menu button at the top of this page, then click the button labeled Power On/Off Button.

When you perform a scan, a Scan Confirmation Report prints (if it has been enabled). The Scan Confirmation Report will report a job status of SUCCESS or FAILED.

Try to scan a document. Does the Scan Confirmation Report print?

If the Scan Confirmation Report does not print, perform the following steps at your workstation.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Workflow Scanning]** link.
6. Select **[General]** in the directory tree
7. Select **[On]** from the **Confirmation Sheet** drop down menu and click on the **[Apply]** button.
8. Return to the device and scan another document using the DEFAULT template. View the error message as detailed on your confirmation report.

View the Scan Confirmation Report. If the Report reads FAILED 'Failure transferring job to network server', the scan repository location may be incorrect. Check the following:

1. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Workflow Scanning]** link.
6. Select **[File Repository Setup]** in the directory tree
7. Click on the **[Edit]** box and check the details configured for your Scan Filing Repository.
8. Make any amendments as necessary and try scanning your documents again.

Scanning via FTP

Check that your FTP service is configured properly.

1. Open a command prompt window and on one line type **[FTP]** then enter a space, then **[IP Address of your FTP Server]**. Press Return.
2. At the 'User' prompt enter the **[user name]** for the account you created for the device scanner.
3. At the 'Password' prompt enter the **[password]** for the account you created for the device scanner.
4. This user account should be able to log in. If you cannot log in as this user check that your FTP server setups have Read/Write access enabled. Ensure the password is correct. If the user can log in, try copying a file into the scan directory to check write access (using get and put commands). Ensure that the FTP server has the Read and Write boxes checked.

Ensure that the user account has full access rights to the scanning directory (repository). Type **[Exit]** to close the command prompt window.

Scanning via NCP (NetWare Core Protocol)

From another workstation log in to the network with the scan user account and password created for the scanning function. Browse to the scan filing location and attempt to create and delete a folder. If you cannot perform this function, check the user account rights.

Scanning via SMB (Server Message Block)

Test the configuration of the scan filing location by attempting to connect to the shared folder (the scan filing location) from another PC, with the user account and password created for the device. Create a new folder within this location and try to delete it. If you cannot perform this function check the user account rights. Verify that the information has been properly set in the Internet Services File Repository Setup page.

Scanning via HTTP(S)

From a TCP/IP networked workstation, test the connection to the web server by Telnet. From a command prompt, start a Telnet session, log in to the device's directory on the web server, and send a POST request and file to the web server. Check to see if the file was received at the repository. If the file was not received, refer to HTTP/HTTPS on page 10-8.

The fault requires further investigation.

Refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: E-mail

If you are experiencing problems with sending an E-mail, first verify the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test page from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Configure your device on the network or resolve any networking issues before attempting to use the E-mail feature.

Ensure E-mail is Installed Correctly

At the device, verify that you have an E-mail button on the device screen interface and that it is not grayed out or unavailable. For instructions to configure the device on the network, refer to Enable TCP/IP and HTTP at the Device on page 2-5.

You may need to press the Services button view the E-mail button on screen.

Install E-mail before proceeding. For instructions refer to E-mail on page 13-1.

> Note
> If you have installed E-mail but the button is grayed out or unavailable, at the device press the Log In / Out button. Enter the Administrator's User Name (default is **[1111]**), touch **[Next]**, enter Password (default is **[1111]**), touch **[Enter]**, touch the Tools tab, and touch User Interface Settings. Touch Service Enablements, then E-mail, set the service to Enable, and touch Save. Reboot the device with the Power On/Off button. For instructions on use of the Power On/Off button, click the Previous Menu button at the top of this page, then click the button labeled Power On/Off Button.

Verify that the E-mail Settings Have Been Correctly Configured on the Device by printing a Configuration Report.

At the Device

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

View the Network Setup details. Verify that the SMTP IP Address is correct and that the TCP/IP Domain Name, Host Name and DNS settings are properly configured.

Was the E-mail Settings Correctly Configured?

For instructions, refer to E-mail on page 13-1.

From a desktop e-mail client, send a test e-mail to the new e-mail account created on the SMTP server for the device. Log in to the mail server with the new account name and password to verify that the e-mail was received at the server.

> Note
>
> A webmail application makes a convenient tool to use to log in to the mail server to check for the receipt of e-mail.

Was E-mail Received at the SMTP Server?

While logged in to the device's e-mail account on the SMTP server, forward the e-mail to yourself.

If you receive the forwarded e-mail, you have verified that a valid path exists for receiving and forwarding e-mail, using the device's account.

If there is still a problem, check for restricted host addresses at the SMTP server that could cause mail to not be received from the device. Other possibilities are that an authentication server is interfering with the device's log in to the mail server, or that the mail client on the device is not working correctly. By successfully sending e-mail to a mail server not subject to authentication, the possibility of a malfunctioning client can be eliminated.

- Is the device's account name and password correct?
- Is the mail server down?
- Check that the mail server is configured to accept SMTP mail, as not all servers are configured to accept SMTP e-mail. The device requires access to a mail server that accepts inbound mail traffic.
- Check for restricted host addresses at the SMTP server. Verify that the device is not a restricted host.
- Try sending an e-mail from the device again. Ask the SMTP administrator to confirm that no errors were encountered and check for 'bounce' messages to the device's "Reply To" address.
- Check that the message size does not exceed the attachment or message size limit policy of your SMTP server.
- Troubleshoot the network path to the SMTP server. It may be necessary to perform a network trace analysis.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: Internet Fax

If you are experiencing problems with sending an Internet Fax, first verify that the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test page from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Configure your device on the network or resolve any networking issues before attempting to use the Internet Fax feature. For Instruction to configure the device on the network, see Enable TCP/IP and HTTP at the Device on page 2-5.

Ensure Internet Fax is installed properly on the device.

At the device, verify that you have an Internet Fax button on the device screen interface and that this is not grayed out and unavailable.

You may need to press the Services button to view the Internet Fax button on screen.

Install Internet Fax before proceeding. For instructions, refer to Internet Fax on page 14-1.

> Note
> If you have installed Internet Fax but the button is grayed out or unavailable, at the device press the Log In / Out button. Enter the Administrator's User Name (default is **[1111]**), touch **[Next]**, enter Password (default is **[1111]**), touch **[Enter]**, touch the Tools tab, and touch User Interface Settings. Touch Service Enablements, then Internet Fax, set the service to Enable, and touch Save. Reboot the device with the Power On/Off button. For instructions on use of the Power On/Off button, click the Previous Menu button at the top of this page, then click the button labeled Power On/Off Button.

Verify that the Internet Fax settings have been correctly configured on the device by printing a Configuration Report.

At the Device

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

View the Network Setup details. Verify that the SMTP Server Address is correct and that the TCP/IP Domain Name, Host Name and DNS settings are properly configured. Verify the POP3 Server Address is correct.

Are the Internet Fax Settings Correctly Configured?

For instructions, refer to Internet Fax on page 14-1.

From a desktop e-mail client, send a test e-mail to the new e-mail account created on the SMTP server for the device. Log in to the mail server with the new account name and password to verify that the e-mail was received at the server.

Note

A webmail application makes a convenient tool to use to log in to the mail server to check for the receipt of e-mail.

Has the Internet Fax (e-mail) been received at the SMTP server?

SMTP items to check

- Is the device's account name and password correct?
- Is the mail server down?
- Ask the SMTP administrator to confirm that no errors were encountered and check for 'bounce' messages to the device's "Reply To" address.
- Check that the message size does not exceed the attachment or message size limit policy of your SMTP server.
- Check that the mail server is configured to accept SMTP mail, as not all servers are configured to accept SMTP e-mail. The device requires access to a mail server that is configured for SMTP.
- Check for restricted host addresses at the SMTP server. Verify that the device is not a restricted host.
- Troubleshoot the network path to the SMTP server. It may be necessary to perform a network trace analysis.

POP3 Errors

If you are experiencing problems with receiving Internet Fax messages at the device, verify the POP3 address details have been properly configured.

At the Device

1. Touch the **[Internet Fax]** button.
2. Enter the Internet Fax address of the device (the E-mail address configured within Internet Services).
3. Touch the **[Add]** button, then touch **[Close]**. Place a document in the document handler and press the green start button. The document should be received as an Internet Fax job. If it is not - check the POP3 server address details to make sure they have been properly configured within Internet Services.

Check the operation of the device's SMTP and POP 3 account, as follows:

1. On a network connected workstation, set up e-mail using the same SMTP and POP 3 server and account (with passwords) as the device.
2. Send an e-mail to yourself.
3. If the e-mail arrives at your e-mail in box, you have proven that the device's account for both the SMTP and POP3 server(s) is valid.
4. If there is still a problem, check for restricted host addresses at the SMTP server that could cause mail to not be received from the device. Other possibilities are that an authentication server is interfering with the device's log in to the mail server, or that the mail client on the device is not working correctly. By successfully sending e-mail to a mail server not subject to authentication, the possibility of a malfunctioning client can be eliminated.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: Server Fax

If you are experiencing problems with sending a Server Fax, first verify the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test page from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Note

Server Fax and Embedded Fax are mutually exclusive services. If one is enabled, the other will not function. Perform the steps under "Is the Fax button available on the device," below to check which service is enabled.

Is the Device Functioning on the Network as a Printer?

Configure your device on the network or resolve any networking issues before attempting to use the Server Fax feature. For instructions to configure the device on the network, see Enable TCP/IP and HTTP at the Device on page 2-5.

Ensure Server Fax is Installed Correctly

At the device, verify that you have a Fax button on the device screen interface and that this is not grayed out and unselectable.

You may need to press the Services button to view the Fax button on screen.

Is the Fax Button Available on the Device?

Install Server Fax before proceeding. For instructions, refer to Server Fax on page 23-1.

Note

If you have installed Server Fax but the button is grayed out or the service is unavailable, at the device press the Log In / Out button. Enter the Administrator User Name (default is **[1111]**), touch **[Next]**, enter the Password (default is **[1111]**), touch **[Enter]**, touch the Tools tab, and touch User Interface Settings. Touch Service Enablements, then Server Fax, set the service to Enable, and touch Save. Reboot the device with the Power On/Off button. For instructions on use of the Power On/Off button, click the Previous Menu button at the top of this page, then click the button labelled Power On/Off Button.

Verify that the Server Fax settings have been properly configured on the device by printing a Configuration Report.

At the Device

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

View the Server Fax Setup details. Verify that the Protocol is correct and that the Server Name and Path to the Fax repository settings are properly configured.

Are the Server Fax Settings Correctly Configured?

Configure the Server Fax settings before continuing. For instructions, refer to Server Fax on page 23-1.

Check the Third Party Fax Server Configuration

1. At the fax server, disable the service so that it does not try to collect new faxes from the fax filing repository. This will depend on the particular product but often the relevant service can be stopped. Refer to the manufacturer's instructions contained with the fax server software to complete this task.
2. Send a test fax from the device.
3. View the location on the server where the fax filing repository was created. Verify that a directory with the extension .XSM has been created and contains the correct TIFF files (one per page of the fax sent).

Does the fax filing repository contain the TIFF files?

If the fax filing repository contains the TIFF files then the device has successfully completed its task. The problem lies with the third party fax server. Ensure the server is configured properly and the path to the fax filing repository is set. Refer to the manufacturer's instructions contained with the fax server software to complete this task.

Check the User Account and Fax Filing Location

1. Verify that the user account and password created for the Server Fax feature are correct and have sufficient rights (permissions) to write files and create directories in the directory (the fax filing location).
2. Try logging into the fax filing location from another PC using the device's account and password. Try to create a directory and delete the directory. If you cannot perform this function check the user account permissions.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: Embedded Fax

If you are experiencing problems with Embedded Fax, first verify that the device is functioning in its existing configuration by making a photocopy at the device.

Is the device functioning?

Resolve any mechanical issues before attempting to use Embedded Fax. For assistance and support, refer to the www.xerox.com website.

Note

Server Fax and Embedded Fax are mutually exclusive services. If one is enabled, the other will not function. Perform the steps immediately below, to check which service is enabled.

Ensure Embedded Fax is Installed Correctly

At the Device

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press **<Machine Status>**, then the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch **[Embedded Fax Settings]**.
6. This should read **[Enable]**. If this is not Enabled or the Fax Install screen appears, refer to the instructions to configure Embedded Fax in this guide.

Ensure the Fax Settings are Correctly Configured

Ensure the device has been configured with the correct fax (telephone) number.

At the Device

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press **<Machine Status>**, then the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch **[Fax Service Settings]**.

Verify that all Fax Setting configuration steps have been performed. Refer to Embedded Fax on page 15-1.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: Network Accounting

If you are experiencing problems with Network Accounting, first verify that the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test page from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Is the Device Functioning on the Network as a Printer?

Configure your device on the network or resolve any networking issues before attempting to use the Network Accounting feature. For instructions to configure the device on the network, see Enable TCP/IP and HTTP at the Device on page 2-5.

Ensure Network Accounting is installed correctly

At the device, press the Services button and touch any button on the screen interface.

Does the device ask you for a User Name and Account?

Verify that Network Accounting is installed and enabled before proceeding

To verify that Network Accounting is installed, print a Configuration Report and look under Installed Options to see the status of Network Accounting.

To print a Configuration Report, at the device press the Machine Status button. touch Print Reports, touch Configuration Report, touch Print Selected Report, then touch Close.

For instructions to both install and enable the Network Accounting feature, refer to Network Accounting on page 20-1. Note that Network Accounting can be installed, but not enabled.

Finally, try rebooting the device with the Power On/Off button. For instructions on use of the Power On/Off button, click the Previous Menu button at the top of this page, then click the button labelled Power On/Off Button.

Test Communication between the Network Accounting Server and the Device

At your network accounting server:

1. Open the web browser and enter the *IP address* of the device in the address bar, and press **[Enter]**.
2. The device's Internet Services web pages should appear. It they do not, verify the IP address settings on the device. If you do not have a web browser, test connectivity by pinging the IP address of the device from your Network Accounting server.
3. Verify that your network accounting server is configured properly. Consult the manufacturer's documentation with your network accounting server to perform this task.

Dynamic IP Addressing and Network Accounting

If Dynamic TCP/IP addressing is used, be sure to set lease times long enough on the DHCP server to allow for normal maintenance shutdowns. If your device suddenly stops communicating with the network accounting solution, print a Configuration Report to check TCP/IP settings to be sure that they have not changed. Also, verify, by pinging, that the server's settings have not been changed.

At the Device

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Power On/Off Button

The Power On/Off button is located on the right front of the device. Press the button to the On (I) position to power on the device. If the device does not show signs of powering on, (with lights flashing on the user interface, for example), check the circuit breaker and power cable located at the lower, right rear of the device. The circuit breaker must be set to the On (I) position. The power cable must be plugged in to the device, as well as to a live source of electric power.

When switching off the device, press the button to the Off (O) position. The printer will power off quickly, however for the system to be fully powered off you must observe the network activity light on the Controller at the rear of the device. When the network activity light stops blinking, the Controller has shut off and the entire system is powered off.

Font Management Utility and Unicode

A Unicode font kit is available for this device. Installation of the Unicode fonts, per the kit's instructions, provides the required character sets to print documents in multiple languages, in an SAP printing environment. To order the kit, contact your Xerox representative.

The CentreWare Font Management Utility is used to manage fonts on one or more printers.

The management process involves downloading soft fonts to your printer(s). For example, you may have a logo or graphic that uses a particular font. By downloading the font to a printer, you can print the logo or graphic with the appropriate typeface and other attributes, such as weight and colour. Downloading fonts to printers can also improve printing performance and reduce network traffic.

Downloaded fonts may then be added, deleted or exported to a file. The utility also allows you to add or delete printers or view printer lists.

The utility is available at no cost from the Support and Drivers section of www.xerox.com.

Unicode

Xerox Unicode 3.0 for SAP fonts will enable printing Japanese, Korean, and Chinese characters from SAP using the following fonts:

ANMDJ.ttf Andale Mono WT J(Japanese version)

ANMDK.ttf Andale Mono WT K(Korean version)

ANMDS.ttf Andale Mono WT S(Simplified Chinese version)

ANMDT.ttf Andale Mono WT T(Traditional Chinese version)

Unicode uses the Font Management Utility.

Refer to your Xerox Representative for further information.

Index

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X